LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

CITRIX-JULKAISUJÄRJESTELMÄN VALVONTA

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Kalle Suuronen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

SUURONEN, KALLE: Citrix-julkaisujärjestelmän valvonta

Tietoliikennetekniikan opinnäytetyö, 94 sivua, 76 liitesivua

Kevät 2015

TIIVISTELMÄ

Tämän työn tavoitteena on olla ohjeistavana työnä DNA Oy:n Citrix-julkaisujärjestelmän valvonnalle ja toteuttamiselle hyödyntämällä Citrix EdgeSight- ja Microsoft System Center Operations Manager -valvontajärjestelmiä. Työn keskiössä on useasta järjestelmästä koostuva Citrix-julkaisujärjestelmä. Julkaisujärjestelmän tarkoituksena on tarjota käyttäjille virtualisoituja ohjelmia ja työpöytiä vaivattomasti ja tietoturvallisesti paikasta, laitteesta tai käyttöjärjestelmästä riippumatta.

Virtualisoinnin eri osa-alueet ovat vahvasti esillä suurten yritysten toiminnoissa ja niiden tehostamisessa. Palvelin-, tallennustilan virtualisointi ja verkon virtualisointi on ollut pidempään jo osana yritysten sisäisiä ja ulkoisia palveluja. Sovellus- ja työpöytävirtualisoinnin kokonaisvaltainen hyödyntäminen on ollut vielä vähäistä verrattaen perinteisempiin virtualisointitapoihin kuten palvelinvirtualisointiin.

Citrix Systems on virtualisointi-infrastruktuuriin keskittyvä yritys, joka tarjoaa sovellus- ja työpöytävirtualisointiin tarkoitetettuja tuotteita, kuten Citrix XenApp ja XenDesktop. Citrix-julkaisujärjestelmän toiminta perustuu keskeisesti näihin tuotteisiin ja Citrixin oman ICA-protokollan toimintaan. Citrix-julkaisujärjestelmä myös hyödyntää toiminnassaan muita järjestelmiä kuten Microsoft App-V, ja vaatii toimiakseen kattavan infrastruktuurin. Citrix-julkaisujärjestelmän valvonnassa hyödynnetään keskeisiä verkonvalvontatekniikoita: SNMP ja WMI. Tekniikoiden avulla saadaan tärkeää informaatiota järjestelmien toiminnasta.

Käytännön työssä keskityttiin pääosin Microsoft System Center Operations Manager -valvontajärjestelmään. Käytännön osuudessa käydään läpi valvontajärjestelmän käyttöönottoa ja määrityksiä, joita voidaan soveltaa Citrix-julkaisujärjestelmän valvonnassa. Määrityksiä tehdään valvonnan, automaation ja tietoturvan osalta. Määrityksien avulla valvontajärjestelmä voidaan ottaa kattavasti käytäntöön. Citrix tarjoaa myös oman EdgeSight-valvontajärjestelmän, joka lopuksi integroitiin osaksi yhtenäistä valvontakokonaisuutta.

Asiasanat: virtualisointi, verkonvalvonta, Citrix, Microsoft System Center Operations Manager, XenApp, XenDesktop, EdgeSight

Lahti University of Applied Sciences
Degree Programme in Information Technology

SUURONEN, KALLE: Monitoring of the Citrix publishing system

Bachelor's Thesis in Telecommunications, 94 pages, 76 pages of appendices

Spring 2015

ABSTRACT

The main goal of this thesis was to examine how two network monitoring systems, Microsoft System Center Operations Manager and Citrix EdgeSight, can be utilized in monitoring DNA Oy's Citrix publishing system. The thesis deals with technologies and systems around the Citrix publishing system. The main goal of the Citrix publishing system is to offer users virtualized applications and desktops effortlessly and securely despite of location, hardware or operating system.

Different fields of virtualization are strongly visible in optimizing the operations of big enterprises. For years, server, storage and network virtualization have been part of internal and external services of companies. Utilizising of application and desktop virtualization has been minor compared to more traditional ways to virtualize, such as server virtualization.

Citrix Systems is a company that focuses on infrastructure virtualization and offers application and desktop virtualization products like Citrix XenApp and XenDesktop. The operation of the Citrix publishing system focuses strongly on these products and the operation of the Citrix ICA protocol. In its operation, the Citrix publishing system also utilizes a variety of other systems, for example Microsoft App-V. The Citrix publishing system also requires a comprehensive infrastructure to work on. In the monitoring of the Citrix publishing system, essential monitoring technologies are used: SNMP and WMI. Using these technologies makes essential monitoring information gathering possible.

The practical work focused mainly on the Microsoft System Center Operations monitoring system. After installation, several configurations were made on the monitoring system, which can be adapted on monitoring the Citrix publishing system. Configurations were made to instruct how to monitor, automate and keep your monitoring system secure. With these configurations it is possible to deploy the monitoring system. Citrix also offers its own EdgeSight monitoring system, which is an integrated part of the bigger monitoring system.

Key words: virtualization, network monitoring, Citrix, Microsoft System Center Operations Manager, XenApp, XenDesktop, EdgeSight

SISÄLLYS

LYHENNELUETTELO

AD	Active Directory. Microsoftin hakemistopalvelu ja käyttäjätietokanta. AD mahdollistaa keskitetyt resurssit.
CIM	Common Information Model. Avoin standardi, jolla määritetään, millä tavalla laitteiden hallittavat elementit voidaan ilmentää olioina ja luoda riippuvuuksia niiden välille.
CGP	Common Gateway Protocol. Tunnelointiprotokolla, joka käyttää TCP-porttia 2598.
DAS	Direct Attached Storage. Digitaalinen media, kuten ulkoinen kiintolevy, joka on suoraan kiinni tietokoneen raudassa.
DCOM	Distributed Component Object Model. Microsoftin teknologia, jolla voidaan keskustella useiden verkossa olevien koneiden kanssa.
DHCP	Dynamic Host Configuration Protocol. Protokolla, joka mahdollistaa Internet Protocol -osoitteiden automaattisen jaon tietokoneille.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä, joka mahdollistaa verkkotunnuksien liittämisen numeeriseen Internet Protocol -osoitteeseen.
EUEM	End User Experience Monitoring. Citrixin ICA-protokollan sisällä olevia suorituskykylaskureita, jotka mittaavat käyttäjäkokemusta.
FQDN	Fully Qualified Domain Name. Tietokoneen kokonainen domain-nimi.

HDX	High Definition eXperience. Joukko Citrixin teknologioita, jotka tarjoavat korkealaatuisen käyttäjäkokemuksen sovellusvirtualisoinnissa.
HTTP	Hypertext Transfer Protocol. Protokolla, joka huolehtii tiedonsiirrosta selaimen ja WWW-sivustojen välillä.
HTTPS	Hypertext Transfer Protocol Secure. Sama kuin HTTP-protokolla, mutta salaa istunnon.
ICA	Indepenedent Computing Architecture. Citrixin oma esitystapavirtualisointiin tarkoitettu protokolla.
ICMP	Internet Control Message Protocol. Protokolla, jota käytetään verkon diagnosointiin.
IMA	Independent Management Architecture. Citrixin oma arkkitehtuuri, joka luo kehyksen palvelinten kommunikointiin.
IPMI	Intelligent Platform Management Interface. Tietokoneen rajapinta, jota hyödyntäen tietokonetta voidaan hallita tai kerätä tietoa.
ISCSI	Internet Small Computer System Interface. Protokolla, joka määrittää, kuinka paketit siirretään TCP/IP-verkossa.
LVM	Logical Volume Manager. Hallintaohjelma, jolla voidaan Linuxissa hallita kovalevyjä.
MIB	Management Information Base. SNMP-protokollan toimintaan perustuva tietokanta, johon tallennetaan laitteiden tietoja.
MOF	Managed Object Format. Syntaksi, jota hyödynnetään WMI-rajapinnassa tiedon esittämisessä.

MPLS	Multi Protocol Layer Switching. Tekniikka, joka kuljettaa ja kapsuloi sisäänsä useita protokollia verkossa.
NAS	Network Attached Storage. Verkkolevy, joka tarjoaa pääsyn tiedostoihin lähiverkosta.
NFS	Network File System. Sun Microsystemsin kehittämä tiedonsiirtoprotokolla verkkoon.
OID	Object Identifier. SNMP-protokollan MIB-tietokannassa olevia olioiden nimiä tai tunnisteita.
OSI ja	Open System Interconnection Model. Standardoitu seitsemän kerroksen malli tiedonsiirtoon, joka kertoo, kuinka protokollat ohjelmat voivat viestiä verkossa.
RDP	Remote Desktop Protocol. Microsoftin protokolla, jonka tehtävä on esittää kuvainformaatiota käyttäjälle.
SaaS	Software as a Service. Tekniikka, jolla käyttäjälle tuodaan ohjelmisto palveluna.
SAN	Storage Area Network. Arkkitehtuuri, joka mahdollistaa verkkolevyjen yhdistämisen palvelimiin paikallisina levyinä.
SCOM	System Center Operations Manager. Microsoftin infrastruktuurin valvontaan tarkoitettu valvontajärjestelmä.
SMB	Samba. Protokolla, joka mahdollistaa tiedonsiirron ja tulostuspalvelut verkossa.
SNMP	Simple Network Management Protocol. Protokolla, joka mahdollistaa laitteiden hallinnan ja valvonnan verkossa.
SOAP	Simple Object Access Protocol. XML-pohjainen viestintäprotokolla, joka mahdollistaa järjestelmäriippumattoman kommunikoinnin.

SSL	Secure Sockets Layer. Standardoitu tekniikka, joka mahdollistaa salatun istunnon asiakkaan ja palvelimen välillä.
SQL	Structured Query Language. Ohjelmointikieli, jonka avulla voidaan lukea ja hallita tietoa relaatiotietokannoista.
TCP	Transmission Control Protocol. Internet Protocol -verkon keskeisin tiedonsiirtoprotokolla, joka mahdollistaa luotettavan tiedonsiirron. Luo yhteyden osapuolten välille.
UDP	User Datagram Protocol. Tiedonsiirtoprotokolla, joka ei luo yhteyttä osapuolten välille.
WBEM	Web-Based Enterprise Management. Kokoelma tietokoneiden hallinnoimiseen tarkoitettuja tekniikoita.
WinRM	Windows Remote Management. Microsoftin toteutus tietokoneiden etähallintaan.
WMI	Windows Management Instrumentation. Infrastruktuuri hallintadatalle ja toiminnoille Windows-käyttöjärjestelmissä.
VDI	Virtual Desktop Infrastructure. Työpöytävirtualisointi, tekniikka, jolla käyttäjän työpöytäympäristö erotetaan fyysisestä laitteesta.
VLAN	Virtual Local Area Network. Fyysisestä verkosta eriytetty ohjelmallisesti yksi tai useampi erillinen looginen verkko.
VPN	Virtual Private Network. Tekniikka, joka mahdollistaa fyysisten verkkojen yhdistämisen loogiseksi kokonaisuudeksi Internetin yli tietoturvallisesti.
XML	Extensible Markup Language. Merkintäkielien standardi, suunniteltu kuvaamaan tiedoston sisällä olevaa dataa.

1 JOHDANTO

Opinnäytetyö tehdään DNA Oy:lle, joka on suuri suomalainen tietoliikennekonserni. DNA tarjoaa puhe-, data- ja tv-palveluita kuluttajille ja yrityksille. DNA työllisti vuonna 2014 noin 1700 henkilöä ja liikevaihtoa kertyi 833,5 miljoonaa euroa.

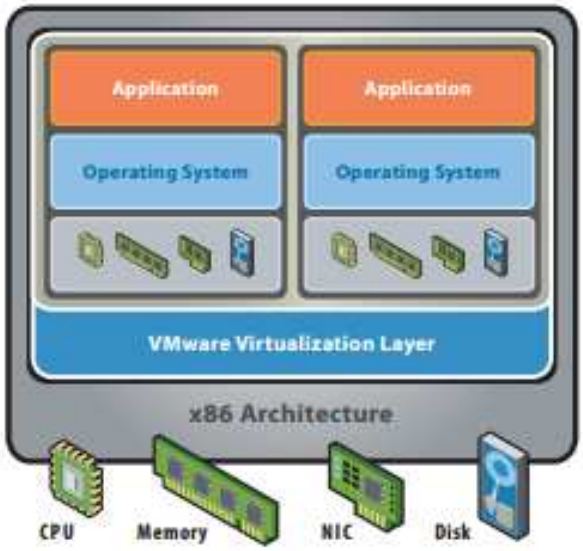
DNA panostaa yhä enemmän mobiilimpaan työskentelytapaan parantamalla etätyöskentelymahdollisuuksia. Panostuksella DNA on jo saavuttanut parannusta henkilöstön työmotivaatiossa ja oman työpanoksen lisäämisessä. Etätyöskentely tuo myös monia muita etuja yritykselle. Yritys voi kasvattaa henkilöstörekrytointipotentiaaliaan, vähentää sairauspoissaolojen määrää ja säästää yleisissä kuluissa, kuten toimitilojen vuokrakuluissa. Etätyöskentelymahdollisuuksia voidaan lisätä usealla tavalla, ja yksi niistä on sovellus- ja työpöytävirtualisoinnin tehokas hyödyntäminen.

DNA hyödyntää Citrix-julkaisujärjestelmää sovellus- ja työpöytävirtualisoinnin toteuttamiseen. Citrix-julkaisujärjestelmän avulla pystytään tarjoamaan turvallinen rajapinta DNA:n ja sen yhteistyökumppaneiden toiminnalle. Citrix-julkaisujärjestelmä kattaa suuren määrän palvelimia ja muita järjestelmiä sisällään. Jotta kokonaisuus toimisi, kaikkien kriittisten komponenttien on toimittava moitteetta. Opinnäytetyö käy läpi yleisiä virtualisointitekniikoita ja keskeisimpiä järjestelmiä, jotka ovat osana Citrix-julkaisujärjestelmää. Opinnäytetyö käsittelee myös verkon- ja palvelinvalvonnan eri tekniikoita ja niitä hyödyntäviä valvonta- ja hallintajärjestelmiä. Opinnäytetyön tavoitteena on julkaisujärjestelmän interaktiivisen valvonnan ohjeistava toteutus Citrix EdgeSight- ja Microsoft System Center Operations Manager -ratkaisuilla, joita voidaan soveltaa Citrix-julkaisujärjestelmän valvonnassa.

2 VIRTUALISOINTI

2.1 Yleistä virtualisoinnista

Virtualisointi pohjautuu fyysisen resurssin esittämiseen loogisena resurssina, jota voidaan jakaa useammalle fyysiselle tai loogiselle resurssille. Fyysisten ja loogisten resurssien välillä sijaitsee virtualisointikerros (KUVIO 1), joka erottelee fyysiset resurssit loogisista ja mahdollistaa useiden loogisten resurssien luomisen ja jakamisen. Yleisin ja tunnetuin tapa virtualisoida on palvelinvirtualisointi, jossa tietokoneella luodaan virtualisointiohjelmalla virtuaalikone, joka vastaa oikeaa fyysistä tietokonetta käyttöjärjestelmineen ja ohjelmineen. Muita mainittavia virtualisoinnin kohteita palvelinvirtualisoinnin ohella ovat sovellusvirtualisointi, työpöytävirtualisointi, tallennustilan virtualisointi ja verkonvirtualisointi. (Vmware 2006; Golden 2011.)



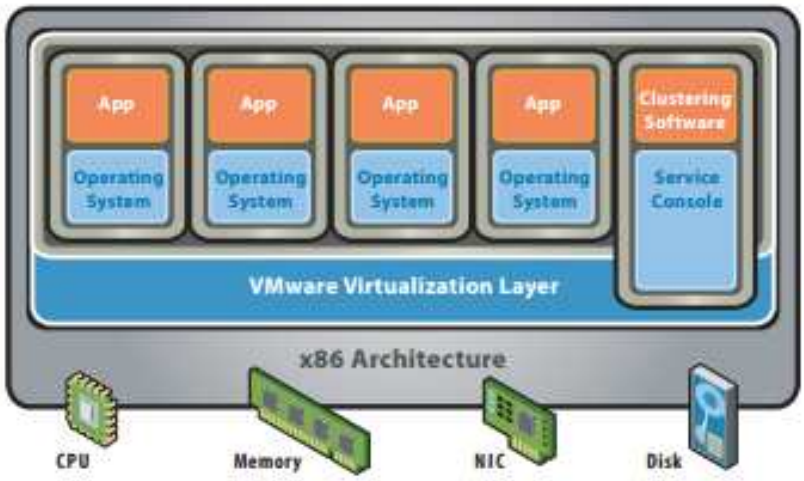
KUVIO 1. Palvelinvirtualisointi (Vmware 2006, 3.)

Virtualisoinnilla voidaan saavuttaa merkittäviä hyötyjä. Esimerkiksi palvelinvirtualisoinnilla voidaan saavuttaa merkittäviä hyötyjä verrattaen tavalliseen fyysiseen x86-arkkitehtuuriin. Olennaisen hyöty palvelinvirtualisoinnista on, että yhdellä fyysisellä palvelimella voidaan ajaa useita virtuaalikoneita ja eri käyttöjärjestelmiä. Palvelinvirtualisoinnilla

pystytään tehostamaan huomattavasti palvelimien käyttöastetta arvioidusta 10-15 prosentista aina 80 prosenttiin asti. Virtualisointi vähentää palvelimien vaatimaa fyysistä tilaa konesaleissa sekä säästää skaalautumisensa vuoksi myös sähkökuluissa. Virtualisoinnin ansiosta IT-ylläpitokustannuksissa voidaan myös säästää keskitetyillä palvelimien hallinnalla. Virtualisointiohjelmistot mahdollistavat myös vikasietoisen ja työnkuormaa jakavan kokonaisuuden. (Golden 2011.)

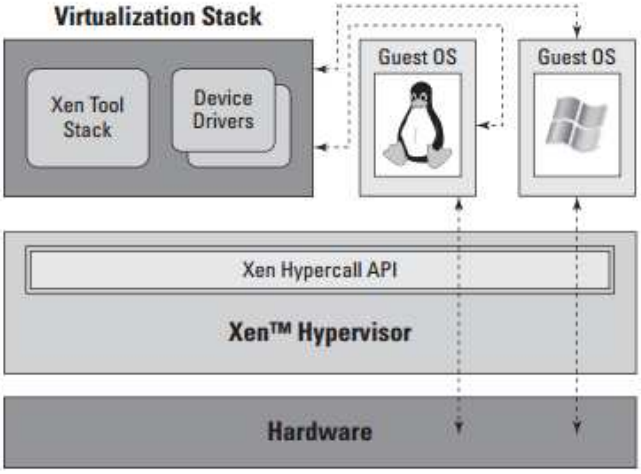
2.2 Palvelinvirtualisointi

Palvelinvirtualisointi voidaan jakaa neljään eri osa-alueeseen: täysvirtualisointiin, paravirtualisointiin, laitteistoavustettuun virtualisointiin ja käyttöjärjestelmätason virtualisointiin. Täysvirtualisointi tapahtuu suoraan fyysisen palvelimen eli hostin raudan päällä (KUVIO 2) käyttäen siihen tarkoitettua virtualisointiohjelmistoa, jota kutsutaan tyypin 1 hypervisoriksi (bare metal). Täysvirtualisoinnissa tyypin 1 hypervisor emuloi koko palvelimen fyysistä rautaa ja on yhteydessä suoraan palvelimen fyysiseen rautaan. Tyypin 2 hypervisori (hosted) sen sijaan toimii käyttöjärjestelmän päällä. Hypervisorin tehtävänä on välittää viestejä virtuaalikoneiden ja palvelimen raudan välillä sekä hallita kokonaisuutta. Täysvirtualisoinnissa virtuaalikoneet eivät ole tietoisia virtualisoinnistaan ja se mahdollistaa laajan tuen eri käyttöjärjestelmille, myös erittäin vanhoille, jotka on kehitetty jo ennen virtualisoinnin tuloa. Huonona puolena täysvirtualisoinnissa voidaan mainita hypervisorin emuloinnista johtuva rasite (overhead), josta aiheutuu pientä viivettä. Suosittuja täysvirtualisointiin pohjautuvia hypervisoreita ovat VMware ESX/ESXi ja Microsoft Hyper-V 2012. (Vmware 2006; Golden & Scheffy 2008.)



KUVIO 2. Täysvirtualisointi (Vmware 2006, 4.)

Paravirtualisointi erottautuu täysvirtualisoinnista jättämällä fyysisen raudan ja hypervisorin välillä olevan emuloinnin tekemättä. Virtuaalikoneet ovat tietoisia virtualisoinnistaan, ja ne ovat yhteydessä suoraan palvelimen rautaan. Paravirtualisointia käyttävä hypervisor koordinoi virtuaalikoneiden pääsyä rautaan (KUVIO 3). Emuloinnin jäädessä pois paravirtualisointia käyttävä hypervisor toimii tehokkaammin kuin täysvirtualisointia käyttävä hypervisor, mikä johtuu virtualisointikerroksen puuttumisesta. Emuloinnin puuttuminen kuitenkin rajaa käytettävien käyttöjärjestelmien määrää. Paravirtualisoinnin hyötyjä on myös tuotu täysvirtualisointia hyödyntävien hypervisoreiden virtuaalikoneisiin asennettavilla lisäpaketeilla. Esimerkkinä paravirtualisoidusta hypervisorista on Xen. (Vmware 2006; Golden 2011.)



KUVIO 3. Paravirtualisointi (Golden 2011, 15.)

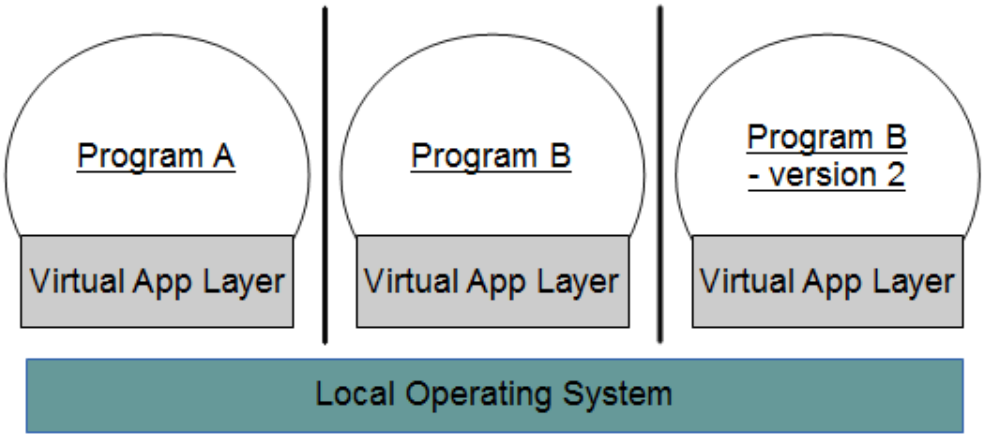
Laitteistoavusteinen virtualisointi perustuu x86-arkkitehtuurin omaavan laitteiston tukemiin käskykantoihin. Käskykantojen tarkoituksena on vähentää hypervisorin overheadia, joka johtuu pääasiassa laitteiston emuloinnista. Suurimmat prosessorivalmistajat Intel ja AMD ovat tuoneet omat käskykantansa prosessoreihinsa: Intel VT:n ja AMD-V:n. Intel VT ja AMD-V ovat yleisiä nimityksiä laitteistoavusteisesta virtualisoinnista, ja ne sisältävät useita eri teknologioita sisälleen. Teknologiat mahdollistavat useita parannuksia virtuaaliympäristössä, kuten paremman hyötysuhteen omaavat hypervisorit, optimaalisemman verkon virtuaaliympäristössä, paremman suorituskyvyn ohjelmille ja virtuaalikoneelle suoraan dedikoidut fyysiset laitteet. Käskykannoilla pystytään parantamaan virtualisointia huomattavasti ja sitä käytetäänkin esimerkiksi täysvirtualisoinnin ja paravirtualisoinnin yhteydessä. (Golden & Scheffy 2008; Intel 2015.)

Käyttöjärjestelmäpohjainen virtualisoinnin lähtökohtana on erillisen käyttöjärjestelmän päällä tapahtuva virtualisointi, kuten tyypin 2 hypervisorilla. Erona tyypin 2 hypervisoriin, virtualisointi tapahtuu käyttöjärjestelmän omalla ytimellä mahdollistaen useiden eristettyjen instanssien suorittamisen. Virtualisoinnin tapahtuessa käyttöjärjestelmän omalla ytimellä se mahdollistaa ainoastaan omasta käyttöjärjestelmästä luodut instanssit eli säiliöt. Linux-käyttöjärjestelmällä voidaan vain ja ainoastaan luoda omia säiliöitä, ei Windows-pohjaisia. Koska instanssien luonti pohjautuu suoraan käyttöjärjestelmän ytimeen, siitä ei aiheudu ylimääräistä overheadia, emulointia ei tarvita ja erillistä käyttöjärjestelmää ei tarvitse asentaa. Tunnettuja ja käytettyjä säiliöitä ovat Solaris Containers, Linux OpenVZ ja FreeBSD Jail. (Golden & Scheffy 2008; Wikipedia 2015c.)

2.3 Sovellusvirtualisointi

Sovellusvirtualisoinnin lähtökohtana on sovellusten tuominen käyttäjien päätelaitteisiin keskitetyiltä palvelimilta, jolloin ohjelmat eivät sijaitse käyttäjän päätelaitteella ja käyttäjien ei tarvitse niistä huolehtia millään tavalla. Sovellusvirtualisoinnissa on kaksi yleistä lähestymistapaa

ohjelmien virtualisointiin. Ohjelmasta voidaan tuoda käyttäjälle pelkästään kuvainformaatiota. Pelkän kuvainformaation lähettämistä käyttäjän päätelaitteelle kutsutaan esitystavan (presentation virtualization) tai istunnon virtualisoinniksi (session virtualization). Vaihtoehtona pelkän kuvainformaation tuomiselle, voidaan sovelluksen data tuoda puskuroimalla eli streamaamalla osittain tai kokonaan käyttäjän päätelaitteelle aina ohjelman käynnistyksen yhteydessä. Tätä tapaa kutsutaan ohjelmien täysvirtualisoinniksi (application virtualization) tai ohjelman streamaamiseksi (application streaming). Monet virtualisointijärjestelmät hyödyntävät toteutuksissaan molempia virtualisointitapoja, jolloin molempien parhaat puolet saadaan hyödynnettyä. Sovellusvirtualisoinnilla voidaan saavuttaa huomattavia etuja yrityksille. Sovellusvirtualisointia hyödyntäen käyttäjät voivat käyttää ohjelmiaan riippumatta sijainnistaan ja käyttöjärjestelmästään. Ohjelmat eivät ole enää sidoksissa omaan käyttöjärjestelmäänsä, mikä lisää huomattavasti käytettävien päätelaitteiden määrää. Virtualisoidut ohjelmat vievät vähemmän prosessorikuormaa päätelaitteelta, jolloin työasemien hankinnoissa voidaan myös säästää. Virtualisoidut ohjelmat ovat toteutustavastaan vuoksi tietoturvallisia. Sovellusvirtualisointi mahdollistaa myös ohjelmista johtuvien IT-ylläpitokulujen pienentymisen, yksinkertaistaen ja nopeuttaen ohjelmien hallintaa ja jakelua. (Citrix Systems, Inc. 2015d; Microsoft 2015b; Wikipedia 2015a.)



KUVIO 4. Täysvirtualisoidut ohjelmat

Esitystapapohjaisessa ohjelman virtualisoinnissa käytetään OSI-mallin esitystapakerrosta virtualisoinnin keinona. Ohjelmia itsessään ei virtualisoida vaan ne sijaitsevat perinteisellä tavalla asennettuina palvelimilla. Käyttäjän käynnistäessään ohjelmaa avataan käyttäjälle oma istunto, jossa esitetään käynnistettävästä ohjelmasta kuvainformaatiota. Käyttäjän näppäimistön painallukset ja hiiren liikkeet lähetetään palvelimelle, minkä jälkeen palvelin lähettää kuvapäivityksiä käyttäjälle. Etuna täysvirtualisoituihin ohjelmiin, voidaan kaikki laskentateho suorittaa palvelimella ja ohjelmia voidaan käyttää useilla eri käyttöjärjestelmillä. Tunnetuimmat istuntopohjaista virtualisointia hyödyntävät tuotteet ovat Citrix XenApp ja Microsoft Terminal Services. Ne pohjautuvat Citrixin Independent Computing Architecture -protokollaan (ICA) ja Microsoftin Remote Desktop Protocol -protokollaan (RDP). (Savill 2012; Citrix Systems, Inc. 2015d.)

2.4 Työpöytävirtualisointi

Työpöytävirtualisointi eli Virtual Desktop Infrastructure (VDI) on tekniikka, jolla käyttäjän työpöytäympäristö erotetaan fyysisestä laitteesta. Käyttäjän virtuaalikone eli työpöytäympäristö sijaitsee hypervisorilla, josta se tuodaan esitystapakerrosta käyttäen käyttäjälle. Kommunikointi virtuaalikoneen kanssa tapahtuu samalla periaatteella kuin istuntopohjaisessa sovellusvirtualisoinnissa. Virtualisoidut työpöydät voivat sisältää valmiiksi asennettuja ohjelmia tai ohjelmat voidaan tuoda käyttäjälle hyödyntäen sovellusvirtualisointia. Työpöytävirtualisointia on mahdollista toteuttaa monella eri tavalla riippuen yrityksen ja käyttäjien tarpeista. Yrityksen näkökulmasta käyttäjien virtuaalikoneet voivat pohjautua yhteen peili-tiedostoon (golden image), josta kaikille käyttäjille voidaan provisioida oma virtuaalikone. Provisioinnilla säästetään huomattavasti levytilaa verrattuna identtisiin kopioihin ja helpotetaan huomattavasti virtuaalikoneiden ylläpitoa. Käyttäjille voidaan myös antaa mahdollisuus asentaa omia ohjelmia ja tallentaa profiilidataa virtuaalikoneeseen liitettävään henkilökohtaiseen virtuaaliseen levyyn. (Golden 2011; Wikipedia 2015b.)

Työpöytävirtualisoinnilla voidaan saavuttaa merkittäviä etuja. Virtualisointi mahdollistaa työn tekemisen paikasta ja laitteesta riippumatta. Työpöytä-virtualisointi lisää myös tietoturvaa, koska työssä käsiteltävä data pysyy koko ajan yrityksen verkossa. Toimistokäytössä työpöytien virtualisoinnilla voidaan säästää rahaa ja tilaa käyttämällä pieniä, edullisia ja energiatehokkaita työasemia, joissa ei ole paikallista kiintolevyä. Työpöytävirtualisointiin tarkoitettuja työasemia kutsutaan nimellä Thin Client. Tavallista työasemaa kutsutaan nimellä Thick Client. Thin Client -työasemat vaativat myös erittäin vähän ylläpidollisia tehtäviä, millä voidaan säästää ylläpitokuluissa. (Golden 2011; Wikipedia 2015b.)

2.5 Tallennustilan virtualisointi

Tallennustilan virtualisoinnilla tarkoitetaan useiden fyysisten levytilojen tai tallennuslaitteiden esittämistä yhtenä loogisena kokonaisuutena. Tallennustilan virtualisoinnin toteuttamiseksi on kolme suosittua tapaa: Storage Area Network (SAN), Network Attached Storage (NAS) ja Direct Attached Storage (DAS). SAN on arkkitehtuuri, jossa yksi tai useampi fyysinen verkkotallennuslaite muodostaa loogisen tallennusjärjestelmäkokonaisuuden verkkoon. SAN-verkon lähtökohtana ei ole tarjota tiedostojärjestelmää verkon yli vaan käyttää lohko-tason toimintoja. SAN mahdollistaa levyjärjestelmän liittämisen suoraan palvelimille niin, että levyjärjestelmä näkyy paikallisena levyjärjestelmänä palvelimella. SAN hyödyntää usein Fibre Channel -teknologiaa tai iSCSI-protokollaa. SAN myös tarvitsee tallennusjärjestelmän hallintaan erillisen hallintalaitteen. NAS eroaa SAN-arkkitehtuurista olemalla yksittäinen verkkotallenuslaite, joka tarjoaa tiedostojärjestelmää suoraan verkon yli tavallisille käyttäjille ja palvelimille. NAS-laitteet käyttävät tiedostojärjestelmänsä jakamiseen tiedostopohjaisia protokollia, kuten NFS:ää tai SMB:tä. DAS eroaa täysin kahdesta aiemmasta virtualisointitavasta ja sitä ei käytetä verkon yli vaan paikallisesti. DAS voi olla käytännössä erillinen laite kovalevyineen liitettynä paikallisesti palvelimeen. Paikallisesti liitetyissä tallenuslaitteissa käytetään yleisesti hyödyksi Logical Volume Manageria (LVM), jonka avulla esimerkiksi

pystytään suurentamaan tai pienentämään loogista levyä tai tiedostojärjestelmää vaikuttamatta ajettavien ohjelmien toimintaan. LVM:ää käytetään yleisesti työpöytäkoneissa sekä palvelimissa. (Bunn, Simpson, Peglar & Nagle 2010; De Luca & Bhide 2010.)

Tallennustilan virtualisoinnilla yhtenä suurimpana etuna on hallinnan yksinkertaistaminen ja helpottuminen. Tiedon määrän kasvaessa jatkuvasti yhä suurempia levyjärjestelmiä tarvitaan ja niiden hallintaan virtualisointi tuo paljon etuja. Toisena erittäin merkittävänä etuna voidaan pitää järjestelmien saatavuutta, jolla voidaan taata jatkuva pääsy yrityksen tärkeään tietoon. Tallenustilojen virtualisoinnilla saavutetaan myös vikasietoisuutta ja saadaan tehostettua tallennustilojen käyttöä. (Bunn, ym. 2010; De Luca & Bhide 2010.)

2.6 Verkon virtualisointi

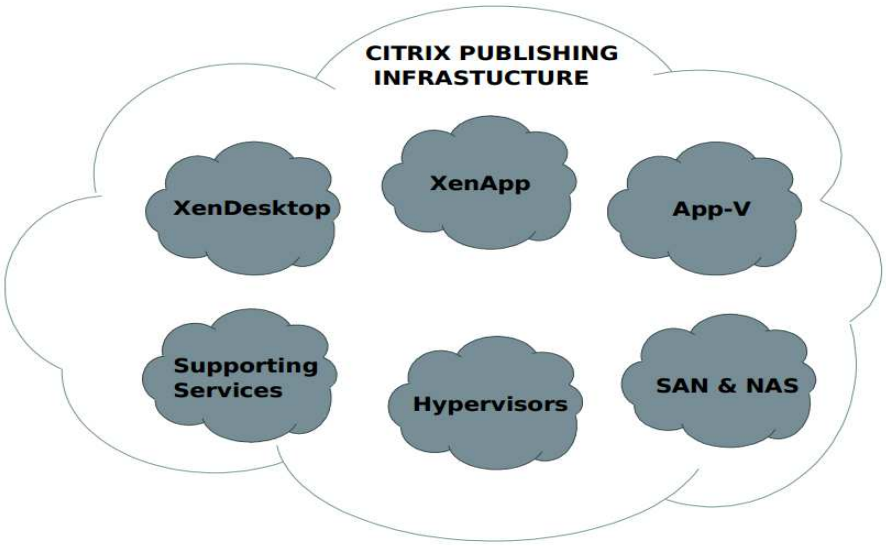
Verkon virtualisointi perustuu OSI-mallin kerroksien eriyttämiseen fyysisestä raudasta. Verkon virtualisointi voidaan jakaa sisäisen verkon virtualisointiin ja ulkoisen verkon virtualisointiin. Verkon ulkoisessa virtualisoinnissa verkon fyysisestä infrastruktuurista muodostetaan ohjelmallisesti kokonaisia tai osittaisia virtuaalisia verkkoympäristöjä, jotka ovat toisistaan eristyksissä. Virtuaalisia verkkoja voidaan luoda käyttäen Virtual Local Area Network (VLAN) -teknologiaa, joka toimii OSI-mallin siirtoyhteyskerroksella. Ulkoisen verkon virtualisoinnissa voidaan käyttää myös Virtual Private Network (VPN) -teknologiaa, jolla voidaan yhdistää yrityksen fyysisiä verkkoja Internetin yli loogiseksi kokonaisuudeksi. VPN toimii OSI-mallin verkkokerroksella. Verkon virtualisoinnissa voidaan vielä käyttää operaattoreiden suosimaa Multi Protocol Layer Switching (MPLS) -teknologiaa, jossa operaattorin runkoverkon läpi voidaan yhdistää asiakkaiden Ethernet-verkkoja ympäri maata yhdeksi paikalliseksi verkoksi (Local Area Network). MPLS-tekniikka sisältää oman toteutuksensa VPN:stä, ja sillä voidaan luoda virtuaalisia reittejä datalle. MPLS-tekniikka hyödyntää OSI-mallin siirtoyhteys- ja verkkokerrosta. (Cisco Systems, Inc. 2009.)

Sisäisen verkon virtualisoinnissa hypervisorin fyysisestä verkkokortista luodaan ohjelmallisesti useita virtuaalisia verkkokortteja, joita voidaan liittää hypervisorilla luotuihin virtuaalikoneisiin. Virtuaalisten verkkokorttien tehtävänä on liittää virtuaalikoneet virtuaaliseen verkkoon virtuaalisen kytkimen avulla. Virtuaalisiin kytkimiin voidaan liittää fyysisiä kytkimiä hypervisorin fyysisen uplink-verkkokortin kautta ja yhdistää fyysiset ja virtuaaliset verkot toisiinsa. Virtuaaliset kytkimet toimivat kuin fyysiset kytkimet, mutta tavallisista virtuaalisista kytkimistä ei löydy fyysisten kytkimien kehittyneimpiä ominaisuuksia. (Vmware 2007.)

3 CITRIX-JULKAISUJÄRJESTELMÄ

Citrix Systems on maailman johtava yritys virtualisoinnissa, joka on keskittynyt tarjoamaan yrityksille ja palveluntarjoajille verkkoratkaisuja, työasemavirtualisointituotteita, sovellusvirtualisointituotteita, palvelinvirtualisointituotteita, pilvipalveluita sekä Software as a Service -palveluita (SaaS). Yrityksen liikevaihto oli vuonna 2013 2,9 miljardia dollaria, ja yrityksen tuotteita käytetään yli 330 000 organisaatiossa ympäri maailmaa. Käyttäjiä Citrixin tuotteilla on yli 100 miljoonaa ympäri maailmaa. Tunnettuja Citrixin tuotteita ovat työpöytävirtualisointiin XenDesktop, sovellusvirtualisointiin XenApp, palvelinvirtualisointiin XenServer ja verkkoratkaisuihin NetScaler. (Citrix Systems, Inc. 2015b.)

Citrix-julkaisujärjestelmä voidaan mieltää yhtenä suurena loogisena kokonaisuutena (KUVIO 5). Citrix-julkaisujärjestelmän infrastruktuuri käsittää alleen monta eri järjestelmää palvelineen sekä palveluineen. Citrix-julkaisujärjestelmän tehtävänä on tarjota vaivattomasti ja tietoturvallisesti käyttäjille käyttöjärjestelmästä, laitteesta tai paikasta riippumattomia virtualisoituja ohjelmia ja virtuaalityöpöytiä. Julkaisujärjestelmä koostuu Citrix XenApp- ja XenDesktop-tuotteiden ympärille, jotka tukeutuvat toiminnassaan muihin järjestelmiin ja palveluihin.



KUVIO 5. Citrix-julkaisujärjestelmän yleiskuva

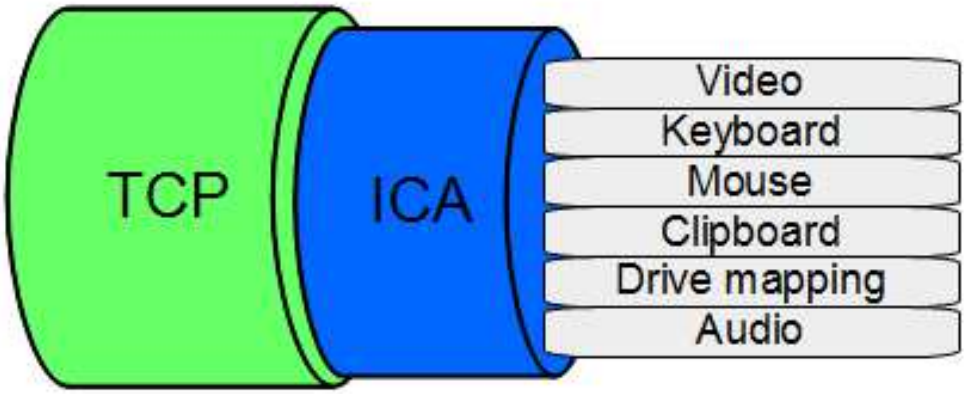
3.1 Citrix Independent Computing Architecture

Independent Computing Architecture (ICA) on Citrixin suunnittelema oma sovelluskohtainen protokolla, joka on Citrixin työpöytä- ja sovellusvirtualisoinnin peruskivi. ICA-protokolla on erittäin kevyt protokolla, joka on suunniteltu käytettäväksi Internetin yli suurilla viiveillä. Esitystapakerroksella toimivat protokollat varmistavat, että sovelluksille menevä tieto, kuten tekstit, kuvat, videot ja äänet, on tarkoituksenmukaista ja tieto voidaan tarvittaessa muuntaa toiseen tiedostomuotoon. Esitystapakerros antaa myös mahdollisuuden tiedon salaukseen ja pakkaukseen. (Wikipedia 2014; Harder & Maynard 2015.)

ICA-protokollaa käytetään ICA-clientin ja palvelimen väliseen liikenteeseen tuomaan käyttäjän työpöydälle virtualisoitu ohjelma hyödyntäen sovellusvirtualisoinnin esitystapavirtualisointia. ICA-protokolla käyttää Transport Control Protocol (TCP) -porttia 1494 natiivisti palvelinfarmin päässä. Jos yhteyden salaus halutaan ottaa käyttöön, voidaan ICA-protokolla tunneloida Common Gateway Protocollan (CGP) sisällä. CGP-protokollan tarjoamaa Secure Socket Layer (SSL) -salausta kutsutaan yhteyden luotettavuudeksi (Session Reliability), ja se käyttää TCP-porttia 2598. (Wikipedia 2014; Harder & Maynard 2015.)

ICA-protokollan yhteys muodostetaan asiakasohjelmalla avaamalla Citrix-järjestelmältä vastaanotettu ICA-tiedosto, joka muodostaa ICA-yhteyden palvelimelle. ICA-protokollan yhteys koostuu maksimissaan 32 virtuaalisesta kanavasta, joilla jokaisella on oma tehtävänsä. Virtuaalisissa kanavissa kulkee informaatiota, joka liittyy esimerkiksi ääneen, kuvaan, näppäimistön ja hiiren painalluksiin, tulostukseen, leikepöytään ja käyttäjäkokemukseen (KUVIO 6). ICA-protokolla käyttää toiminnassaan palvelunlaadun varmistusta, jonka avulla virtuaalisille kanaville voidaan määrittä oma prioriteetti. Palvelunlaadun varmistamisen ohella ICA-protokolla pakkaa tarvittaessa tietoa pienempään, jos kaistanleveys pienenee. ICA-protokolla sisältää uudelleenohjauksen USB-laitteille, Adoben flashille ja äänelle. ICA-protokolla mahdollistaa myös Thin clientillä olevien laitteiden, kuten paikallisten levyjen, äänikortin tai

tulostimien, hyödyntämisen virtualisoitavissa ohjelmissa tai työpöydillä. (Citrix Systems, Inc. 2014a; Harder & Maynard 2015.)



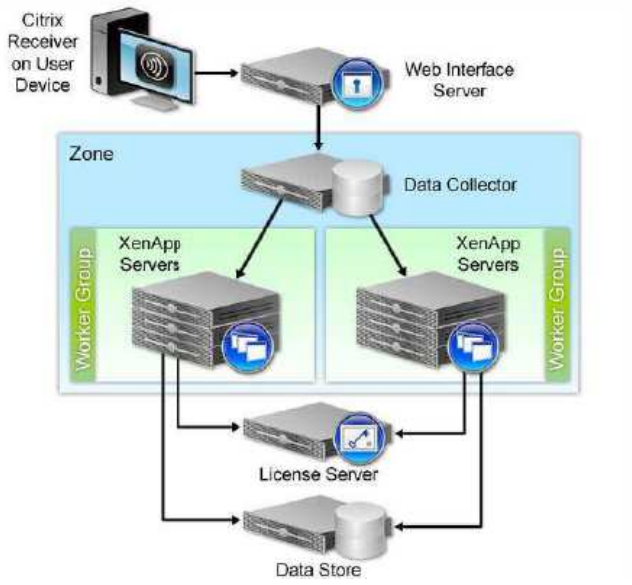
KUVIO 6. ICA-protokollan virtuaaliset kanavat

ICA-protokollan toimintaa on kohenneltu Citrix High Definition eXperience (HDX) tekniikalla. HDX on käytännössä kokoelma eri tekniikoita, joiden tarkoituksena on parantaa käyttäjäkokemusta. Käyttäjäkokemuksen parantamiseen HDX hyödyntää olemassaolevia tekniikoita, kuten uudelleenohjausta, mukautuvaa datan pakkausta ja datan duplikaattien eliminointia verkon liikenteessä käyttäen multicastia ja välimuistia. HDX-tekniikalla pystytään vähentämään kaistan käyttöä ja parantamaan skaalautuvuutta palvelimien puolella. HDX-tekniikalla voidaan tarjota graafisesti vaativia 3D-ohjelmia, kuten suunnitteluun tarkoitettuja ohjelmia käyttäjälle hyvällä käyttäjäkokemuksella. (Citrix Systems, Inc. 2014b.)

3.2 Citrix XenApp 6.5

Citrix XenApp on sovellusvirtualisointiin tarkoitettu järjestelmä, joka mahdollistaa istuntopohjaiset ja täysvirtualisoidut ohjelmat. Citrix XenApp järjestelmän virtualisoituja resursseja on mahdollista käyttää usealla eri laitteella ja käyttöjärjestelmällä: Windows, Mac, Linux, UNIX, DOS, Java ja kaikilla yleisimmillä mobiilikäyttöjärjestelmillä. Käyttäjille virtualisoitavat ohjelmat voidaan toteuttaa usealla eri tavalla ja soveltaa sovellusvirtualisoinnin molempia osa-alueita. XenApp-palvelimia käytetään istuntopohjaiseen virtualisointiin. Täysvirtualisointiin käytetään joko Citrix

Profiler -palvelinta tai Microsoft App-V -järjestelmää. Citrix suosittaa Microsoft App-V:n käyttöä omissa toteutuksissaan. XenApp-järjestelmä tärkeimmät komponentit (KUVIO 7) ovat XenApp-palvelin, kontrolleri (data collector), SQL-tietokanta (data store), lisensointipalvelin ja web-käyttöliittymä-palvelin. Käyttäjät käyttävät selainta ja Citrix Receiver -asiakaspään-ohjelmaa järjestelmän ja heille osoitettujen resurssien hyödyntämiseen. (Musumeci 2012.)



KUVIO 7. XenApp-järjestelmä infrastruktuuri (Shabaz 2014.)

Citrix XenApp pohjautuu Independent Management Architecture (IMA) -arkkitehtuuriin, joka toimii kehyksenä ja määrittää palvelimien välillä tapahtuvan liikenteen XenApp-ympäristössä. IMA on myös yksi tärkeimmistä XenApp-palvelinten tärkeistä Windows-palveluista. IMA-palvelu on käytössä jokaisessa XenApp-palvelimessa ja mahdollistaa keskitetyn hallinnan sekä toiminnalliset alijärjestelmät, jotka ovat välttämättömiä ohjelmiston toiminnallisuudelle. IMA-palvelu mahdollistaa kommunikoinnin palvelimien kesken. XenApp pohjautuu toiminnassaan Citrixin ICA-protokollaan. (Ramlal & Card 2006.)

XenApp-palvelimet toimivat omissa työskentelyryhmissään, joiden avulla voidaan hoitaa esimerkiksi vikasietoisuutta ja kuormantasausta. XenApp-järjestelmää käyttöönotettaessa luodaan oma XenApp-ympäristö, farmi, johon palvelimet liitetään osaksi loogista kokonaisuutta. Farmin avulla

saadaan hallinta keskitettyä yhden yksikön alle. XenApp-ympäristö voi myös sisältää alueita, joiden tarkoitus on yhdistää maantieteellisesti erillään olevia palvelimia loogiseksi kokonaisuudeksi. XenApp-järjestelmää hallitaan ensisijaisesti AppCenter-hallintakonsolin kautta. (Musumeci 2012.)

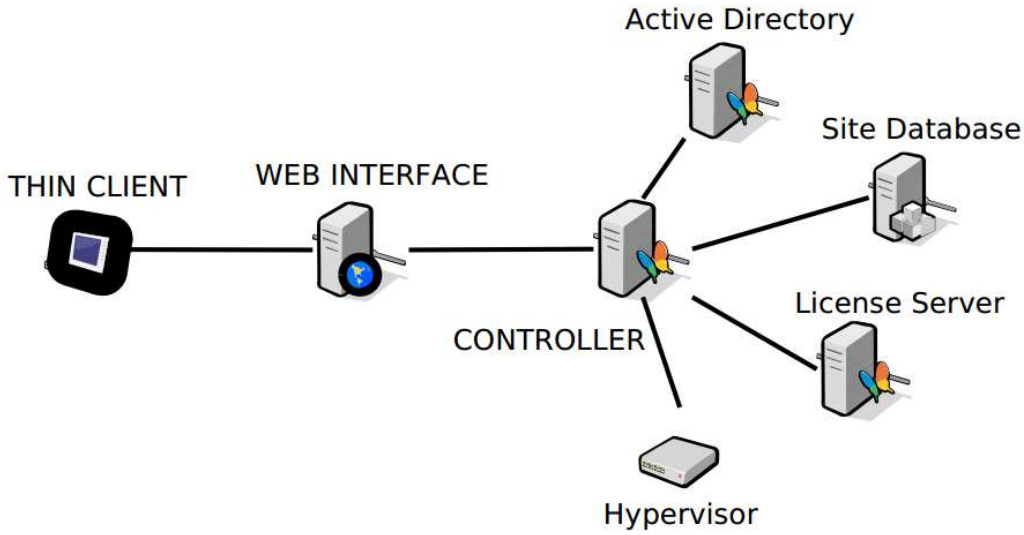
3.3 Citrix XenDesktop 5.6

XenDesktop on Citrixin työpöytävirtualisointiin tarkoitettu järjestelmä, joka XenApp-järjestelmän mukaan pohjautuu toiminnassaan vahvasti ICA-protokollaan. XenDesktop käyttää Citrixin omaa FlexCast-teknologiaa, jonka tarkoituksena on tunnistaa käyttäjä, laite ja verkko. FlexCast-teknologian avulla voidaan käyttäjille jakaa turvallisesti virtualisoituja työpöytiä heidän tarpeensa mukaan. XenDesktopilla julkaistavat virtuaalityöpöydät soveltuvat esimerkiksi tiettyä tehtävää suorittaville työntekijöille, jatkuvasti liikkeellä oleville työntekijöille, yhteistyökumppaneille ja jaettuihin työasemiin. Virtuaaliset työpöydät jaetaan käyttäjille esitystapapohjaisesti eli hyödyntäen OSI-mallin esitystapakerrosta. (Citrix Systems, Inc. 2010b; Brennan, Briggs, Shbeilat & Anderson 2012.).

XenDesktop-järjestelmän olennaisimmat komponentit ovat web-käyttöliittymä-palvelin (web interface server), kontrolleri (Desktop Delivery Controller), Citrix-lisensointipalvelin (Citrix License Server) ja tietokanta (Site Database). XenDesktop-järjestelmä voi koostua yhdestä tai useammasta ympäristöstä (XenDesktop Site). Ympäristö määritetään järjestelmän käyttöönoton yhteydessä. XenDesktop-järjestelmän hallintaan ja ylläpitoon käytetään Desktop Studio- ja Desktop Director -ohjelmia. XenDesktop-ympäristön koosta riippumatta tarvitsee XenDesktop ympärilleen toimiakseen verkkopalveluista vähintään Active Directory -palvelimen, Dynamic Hosting Control Protocol (DHCP) -palvelimen, Domain Name Server (DNS) -palvelimen ja Citrix Receiver -asiakasohjelman käyttäjille. Jos käyttöönotettava XenDesktop-ympäristö

on pieni, XenDesktop komponentit voidaan asentaa halutessaan kaikki samalle palvelimelle. (Fujitsu 2011 ; Brennan, ym. 2012.)

XenDesktop-ympäristön voi koostaa yksinkertaisimmillaan XenDesktopin peruskomponenteista ja järjestelmän toiminnalle tärkeimmistä palveluista (KUVIO 8). XenDesktop-järjestelmä voidaan integroida XenApp-järjestelmän kanssa, jolloin käyttäjän virtuaalityöpöydissä voidaan hyödyntää sovellusvirtualisointia. XenApp-järjestelmällä voidaan virtuaalityöpöydille esimerkiksi streamata ohjelmia hyödyntäen ohjelmien täysvirtualisointia, jolloin ohjelmien hallinta on huomattavasti helpompaa.



KUVIO 8. XenDesktop-ympäristö

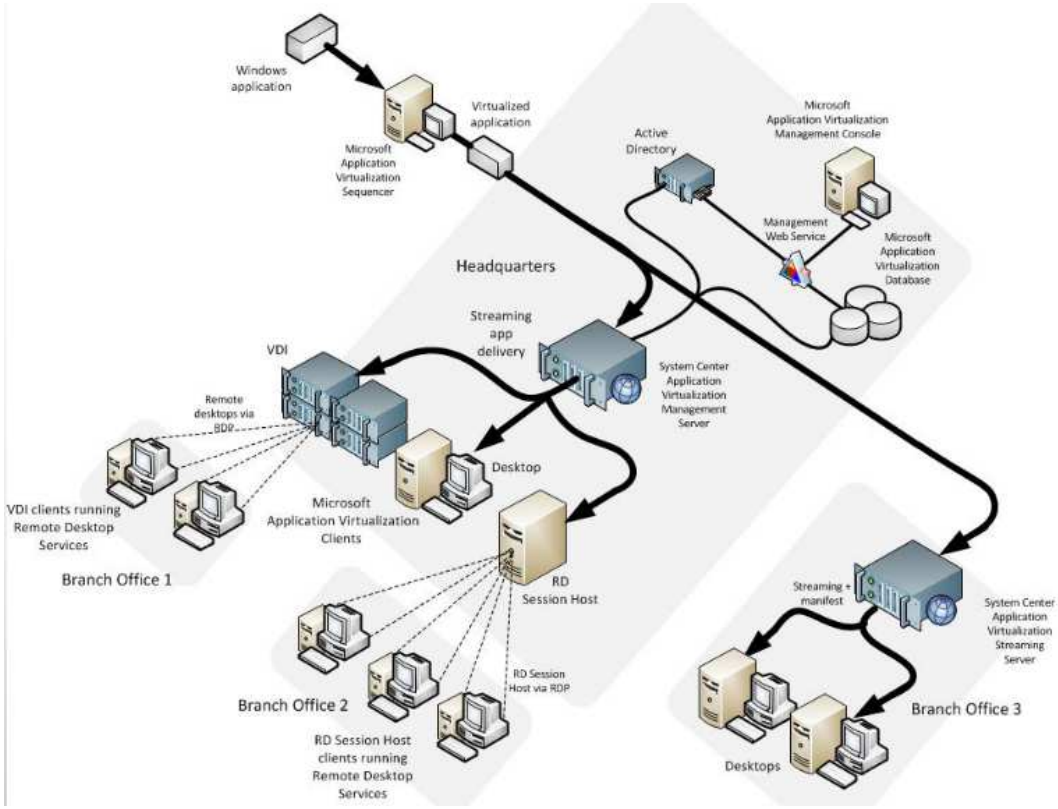
3.4 Microsoft Application Virtualization

Microsoftin tuote sovellusten täysvirtualisointiin on Microsoft App-V. Microsoftin App-V pohjautuu vuonna 2006 sen hankkimaan ohjelmaan nimeltä Soft-Grid, josta Microsoft on kehittänyt oman menestyvän tuotteensa vuosien varrella. App-V toimii ainoastaan Windows-ympäristöissä, ja sillä voidaan virtualisoida lähes kaikkia Windowsin ohjelmia. App-V:tä voidaan hyödyntää Windowsin 32- ja 64-bittisissä ympäristöissä. Microsoft on yhdistänyt uusimpiin App-V-versioihinsa vahvasti PowerShell-komentotulkkiaan, jolla voidaan hoitaa App-V-ympäristön hallintaa ja suorittaa komentosarjoja. Hallintaa voidaan edelleen hoitaa graafisesti.

App-V on kehittynyt yhdeksi oman ohjelmistoalueensa parhaaksi tuotteeksi, ja Citrix onkin siirtynyt käyttämään sitä ensisijaisena vaihtoehtona uudessa XenDesktop 7 -tuotteessaan. (Savil 2012.)

Microsoft App-V -ympäristö tarvitsee toimiakseen useita eri komponentteja. Käyttäjä tarvitsee omalle päätelaitteelleen App-V clientin, jolla käynnistetään streamatut virtualisoidut ohjelmat. Palvelinpuolelle tarvitaan paketointipalvelin (sequencer server), hallintapalvelin (management server), julkaisupalvelin (publishing/streaming server), tietokantapalvelin (SQL server) ja raportointipalvelin (reporting server). App-V-järjestelmän hallintaan tarvitaan hallintapalvelin, jolla kokonaisuutta hallitaan Internet-selaimen avulla käyttäen Microsoft Silverlight -pohjaista hallintakonsolia. Kaikki muutokset ja asetukset tehdään hallintapalvelimen kautta. Tehdyt muutokset järjestelmään tehdään kaikki tietokantapalvelimen sisältämään hallintatietokantaan (Management Database), josta niitä jaetaan muille hallintapalvelimille. (Microsoft 2010; Microsoft 2014.)

App-V-ympäristö on mahdollista toteuttaa kolmella eri tapaa, josta yksinkertaisin toteutustapa on paikallisesti toteutettu (standalone model), joka käsittää ainoastaan paketointipalvelimen ja App-V clientin. Toinen tapa toteuttaa App-V-ympäristö on käyttää streamaus-mallia, jossa käytetään julkaisupalvelimia, paketointipalvelinta ja App-V clienttiä. App-V-komponenttien ohella tarvitaan Active Directorya tai ohjelmistohallintaohjelma julkaisemaan ohjelmien pikakuvakkeet käyttäjille. Ohjelmat ovat virtualisoituja. Kolmas tapa toteuttaa App-V-ympäristö on täyden infrastruktuurin malli (KUVIO 9). Täyden infrastruktuurin malli perustuu App-V-hallintapalvelimiin, joilla hallitaan koko App-V-ympäristöä. Täyden infrastruktuurin mallia käytetään yleensä, kun halutaan käyttää ominaisuuksia, kuten dynaamisia ohjelmajulkaisuja perustuen Active Directoryn käyttäjäryhmiin, tarkentaa ohjelmien lisensoinnin käyttöä ja hyödyntää App-V-raportointia. Kuvion 9 streaming server -palvelin kuvastaa täysvirtualisoitujen ohjelmien verkkolevyä. (Microsoft 2011.)



KUVIO 9. Microsoft App-V täyden infrastruktuurin malli (Microsoft 2011)

3.5 Citrix-julkaisujärjestelmä käyttäjän näkökulmasta

Käyttäjille Citrix-julkaisujärjestelmä ilmenee pääasiallisesti WWW-sivustona, jota käyttäjät hyödyntävät selaimensa avulla. Kaikki käyttäjät tarvitsevat paikalliselle laitteelleen Citrix Receiver -asiakaspään ohjelman, jotta tarvittavat resurssit voidaan tuoda käyttäjälle. Käyttäjät voivat hyödyntää julkaisujärjestelmää kaikilla laitteilla ja käyttöjärjestelmillä, joihin Citrix Receiver -ohjelmisto on ladattavissa. Kun käyttäjät kirjautuvat WEB-rajapintaan (KUVIO 10), heidän käyttöoikeutensa tarkistetaan ja heille oikeutetut resurssit esitetään tavallisina kuvakkeina. Käyttäjät voivat valita haluamansa ohjelman tai työpöydän käynnistettäväksi. Käyttäjät hyödyntävät ohjelmien ja työpöytien virtualisoinnissa Citrix Receiver -ohjelmaa, jonka avulla kuvainformaatio ohjelmasta streamataan käyttäjälle kuvaketta napsauttamalla. Virtualisoituja ohjelmia voidaan käyttää monella tapaa, esimerkiksi paikallisina kuvakkeina, WEB-rajapinnan kautta, Citrix Receiver julkaisuna tai virtuaalityöpöydän sisältäminä.

KUVIO 10. Citrix Web Interface -kirjautumisruutu (Morgan 2015.)

Jos julkaisujärjestelmässä ilmenee joitain ongelmia, ne yleensä ilmevät käyttäjälle esimerkiksi kirjautumisen tai käynnistettävän resurssin hidastumisena, käyttäjän julkaistut kuvakkeet eivät näy, virtualisoidut resurssit eivät käynnisty tai tarvittavat tiedostot eivät aukea. Koska Citrix- julkaisujärjestelmä kattaa sisälleen useita eri järjestelmiä muodostaen kokonaisuuden, asiakas näkee ongelmat yleensä Citrix-ongelmana, vaikka ongelmat saattavat olla jonkin muun järjestelmän toimimattomuutta.

4 VERKONVALVONTA

4.1 Yleistä verkonvalvonnasta

Verkonvalvonta tai verkonhallinta on yleinen termi, jota voidaan toteuttaa hyödyntämällä erilaisia valvontatyökaluja, tekniikoita ja järjestelmiä. Verkonvalvonta ja -hallinta voidaan jakaa useampiin pienempiin osiin: vian-, määritysten-, pääsyn-, suorituskyvyn- ja tietoturvanhallintaan. Verkonvalvonnassa hyödynnetään verkonhallintajärjestelmää, joka on käytännössä palvelin valvontaohjelmistoineen. Valvontajärjestelmää hyödyntäen valvotaan ja hallitaan haluttuja kohteita. (Mauro & Schmidt 2005.)

Verkonvalvontaa hyödyntämällä voidaan saavuttaa merkittäviä etuja yrityksissä. Verkonvalvonnan ja -hallinnan tärkeimpiä etuja ovat palveluiden saatavuuden ja hyvän käyttäjäkokemuksen varmistaminen. Palveluiden toimimattomuuden takia yritys menettää aina rahaa. Toistuvat ongelmat palveluissa työllistävät turhaan yrityksen työntekijöitä ja keskeyttävät työnkulun vaikuttaen negatiivisesti henkilöstön työtehokkuuteen. Palveluissa ulkoisesti näkyvät ongelmat voivat luoda myös negatiivista kuvaa yrityksen toiminnasta. Palveluiden saatavuuden ja käyttäjäkokemuksen varmistaminen voidaan saavuttaa proaktiivisella valvonnalla selvittäen ongelmakohdat yrityksen ympäristössä, tehokkaalla vianetsinnällä ja ratkaisuilla. Valvonnan avulla voidaan myös selvittää oman ympäristön kapasiteettia uusien järjestelmien käyttöönottoa varten. Parhaimmillaan valvonnalla säästetään ylläpitokustannuksissa, maksimoidaan järjestelmäylläpitäjien työpanos ja voidaan skaalata oma ympäristö täysin omien tarpeiden mukaiseksi. (SevOne, Inc. 2015.)

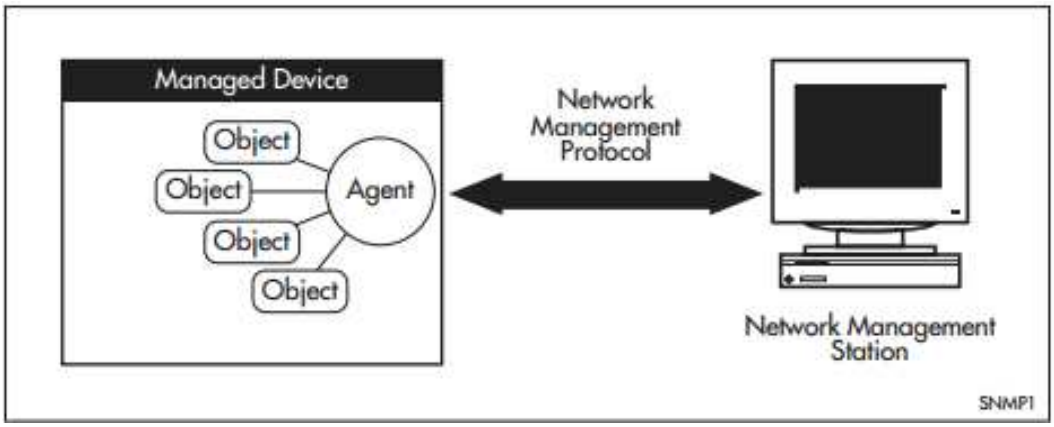
Verkonvalvontaan voidaan mieltää kaikki verkossa kiinni olevat laitteet, kuten tietoliikennelaitteet, palvelimet, työasemat, tulostimet ja levyjärjestelmät. Valvonta voidaan karkeasti jakaa kahteen: palvelinten- ja verkkolaitteiden valvontaan. Verkkolaitteiden, kuten reitittien ja kytkinten valvonnassa ensisijaisesti keskitytään verkkoliitännän tilaan OSI-mallin siirto- ja verkkokerroksilla. Verkkolaitteiden valvonnassa mitataan tavallisesti verkkoliikenteen määrää, laitteen prosessorikuormaa ja

muistinkäyttöä. Palvelinvalvonnassa keskitytään yleisesti palvelimen suorituskyvyn, ohjelmien, prosessien ja palveluiden valvontaan. Palvelimen fyysistä suoriutumista valvotaan tutkimalla palvelimen komponenttien tilaa, joista tärkeimmät valvontakohteet ovat prosessori, keskusmuisti, kovalevy ja virtalähde. Komponentteja valvomalla saadaan esimerkiksi tietoa käyttöasteesta, vikatilanteista ja lämpötiloista. Ohjelmien, prosessien ja palveluiden saatavuutta sekä suorituskykyä voidaan mitata käyttöjärjestelmien rajapintojen kautta hyödyntämällä eri tekniikoita. Käytetyt tekniikat ovat usein kytköksissä laitteen tyyppiin ja käyttöjärjestelmään. Verkon, tietoliikennelaitteiden, Unix-laitteiden ja -palvelinten valvonnassa hyödynnetään ensisijaisesti SNMP-protokollaa. Windows-palvelimien valvonnassa käytetään taas yleisesti Windowsin omaa WMI-arkkitehtuuria, jonka kautta saadaan kattavaa tietoa palvelimen tilasta. Windows-palvelimia on mahdollista valvoa myös SNMP-protokollalla. (Mauro & Schmidt 2005.)

4.2 Simple Network Management Protocol

SNMP-protokolla on suosituin verkonvalvontaan ja -hallintaan tarkoitettu OSI-mallin sovelluskerroksen protokolla. SNMP-protokollaa voidaan käyttää laaja-alaisesti esimerkiksi tietoliikenne- ja tallennuslaitteissa, palvelimissa, työasemissa ja tulostimissa. Tyypillisesti SNMP-protokollaa voidaan hyödyntää selvittämään tietoliikennelaitteiden verkkoliitäntöjen tila, prosessorikuorma, verkkoliikenteen määrä, laitteen lämpötila, vapaan levytilan määrä sekä paljon muuta laitekohtaista tietoa. Protokollasta on julkaistu useita versioita, mutta yleisimmät kolme versiota ovat 1, 2c ja 3. Versio 2c pohjautuu täysin ensimmäiseen versioon tarjoten uusia SNMP-viestejä, yksityiskohtaisempia virheviestejä ja parempia tapoja hakea tietoa. Versioiden 1 ja 2c tieto kulkee selkokielisenä verkossa, ja molemmat versiot ovat yhteisöpohjaisia (community). Uusimman version 3 suurimpana parannuksena aiempiin versioihin on tiedon salaaminen ja eheys sekä yhteisöpohjaisuuden sijasta käyttäjän tunnistaminen. (Allied Telesis 2015; ManageEngine 2015.)

SNMP-protokollan toiminta perustuu kolmen eri komponentin ympärille (KUVIO 11): hallittava laite, verkonhallintalaite ja verkonhallintaprotokolla. Hallittava laite sisältää SNMP-agentin, jonka tehtävänä on kerätä ja tallentaa laitteen tietoja hallintatietokantaansa eli MIB-tauluun (Management Information Base). Agentin tehtävänä on myös tarjota tietoa pyydettäessä verkonhallinta-laitteelle. Agentit lähettävät myös itsenäisesti tietoa merkittävistä tapahtumista (traps) laitteen tilassa verkonhallintalaitteelle. Agenttia on mahdollista käyttää välittämään muiden laitteiden tietoa, jotka eivät tue SNMP-protokollaa. (Allied Telesis 2015.)

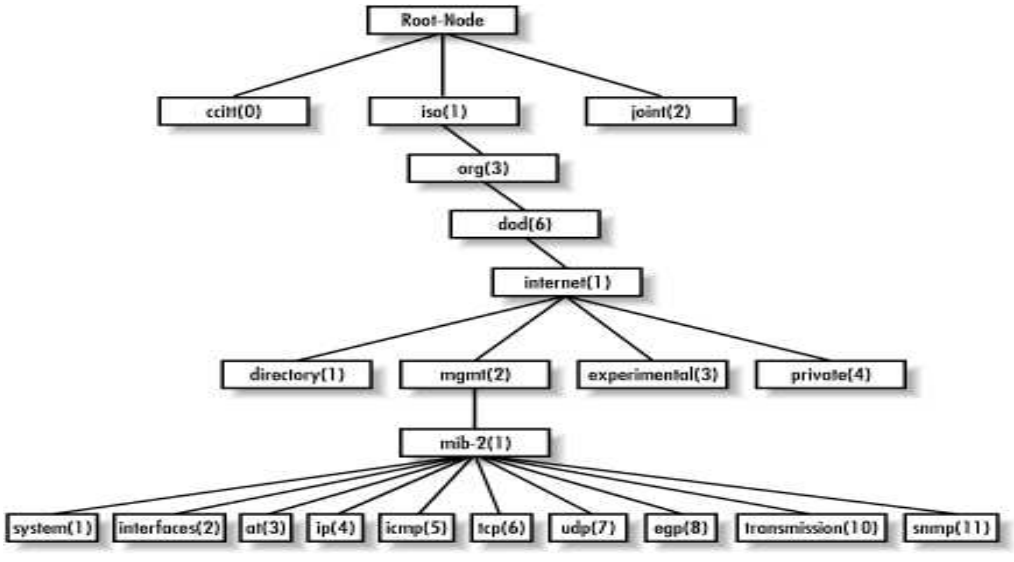


KUVIO 11. SNMP-komponentit (Allied Telesis 2015, 3.)

Verkonhallintalaite on tyypillisesti palvelin, jossa ajetaan verkonvalvonta-ohjelmistoa. Verkonhallintalaitteen avulla voidaan tehdä kyselyitä agenteille, vastaanottaa tietoa agenteilta, tehdä muutoksia laitteen asetuksiin ja kuitata erilaisia tapahtumia agenteilta. Hallittavan laitteen ja verkonhallintalaiteen luottamussuhde toteutetaan joko yhteisöpohjaisesti tai käyttäjätunnistusta hyödyntäen. Yhteisöjä on kolmea eri tyyppiä, jotka on eritelty toisistaan niiden tyypin mukaan: lukuoikeus, luku- ja kirjoitusoikeus sekä ansa. Tyypillisesti lukuoikeus on määritelty julkisena yhteisönä (public), luku- ja kirjoitusoikeus yksityisenä (private) ja ansat erillisenä. Yhteisöille määritetyt nimet ovat käytännössä salasanoja, jotka kulkevat selkokielisenä tekstinä verkossa. Käyttäjätunnistuksessa käyttäjät voidaan tunnistaa symmetrisesti tai käyttämällä yksityistä avainta. Käyttäjien tunnistus tapahtuu salattuna. Käyttäjät voidaan kategorisoida

kolmeen eri ryhmään turvallisuustyyppinsä mukaan: ei tunnistautumista tai yksityisyyttä (noAuthnoPriv), tunnistautuminen ilman yksityisyyttä (authNoPriv) ja tunnistautuminen sekä yksityisyys (authPriv). (Allied Telesis 2015.)

Verkonhallintalaite kerää tietonsa hallittavan laitteen ylläpitämästä MIB-taulusta hyödyntäen SNMP-protokollaa. MIB-taulua voidaan ajatella virtuaalisena tietokantana, joka sisältä linkit hallittaviin olioihin (object). SNMP määrittää mekanismin, jolla tietoa voidaan lukea MIB-taulusta. MIB-taulu on rakenteeltaan puumainen ja hierarkinen (KUVIO 12). MIB-taulun rakenteen määrittely perustuu Structure of Management Information -kehykseen (SMI). MIB-taulussa laitteen paikallisten resurssien esittämiseen käytetään olioiden nimiä eli Object Identifier -tunnisteita (OID). OID-tunnisteet ovat uniikkeja lukuja ja tekstijonoja, joiden esittäminen ja määrittely on myös määrätty SMI:n avulla. Laitteiden MIB-tauluja voidaan lukea erillisillä ohjelmilla tarvittaessa, jos halutaan selvittää jokin laitteen resurssin OID-tunniste. Osa MIB-taulujen OID-tunnisteet ovat standardoitu, mutta jokaisella laitevalmistajilla on kuitenkin omat laitekohtaiset MIB-taulunsa ja OID-tunnisteensa. Kuvion 12 mukaan voidaan OID-tunniste muodostaa liikkumalla MIB-taulussa alaspäin iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1), jolloin OID-muodossa se olisi 1.3.6.1.2.1.1. (Mauro & Schmidt 2005.)



KUVIO 12. MIB-taulu (Mauro & Schmidt 2005, 36.)

SNMP-protokolla hyödyntää toiminnassaan yhteydetöntä OSI-mallin kuljetuskerroksen perustuvaa User Datagram Protocol (UDP) -protokollaa tiedon kuljettamiseen. SNMP perustuu yksinkertaisuudessaan pyyntöihin (GET) ja vastauksiin (SET). SNMP käyttää UDP-porttia 161 lähettämään ja vastaanottamaan pyyntöjä ja porttia 162 vastaanottamaan hallittavien laitteiden tapahtumatietoja. SNMP-protokollan perustoiminnot ja käskyt ovat seuraavat:

- **READ (get-request) –** Luetaan hallittavan laitteen MIB-taulusta muuttujan arvo.
- **WRITE (set-request) –** Muutetaan hallittavan laitteen muuttujien arvoja.
- **TRAP (traps, inform) –** Hallittavat laitteet lähettävät itsenäisesti tietoja laitteessa tapahtuvista muutoksista.
- **Traversal operations (get-next-request, get-bulk-request) –** Komennoilla voidaan selvittää hallittavan laitteen tuettuja muuttujia ja kerätä peräkkäistä tietoa tai vaihoehtoisesti suuri määrä tietoa kerralla MIB-taulusta, kuten reititystaulun informaatio.

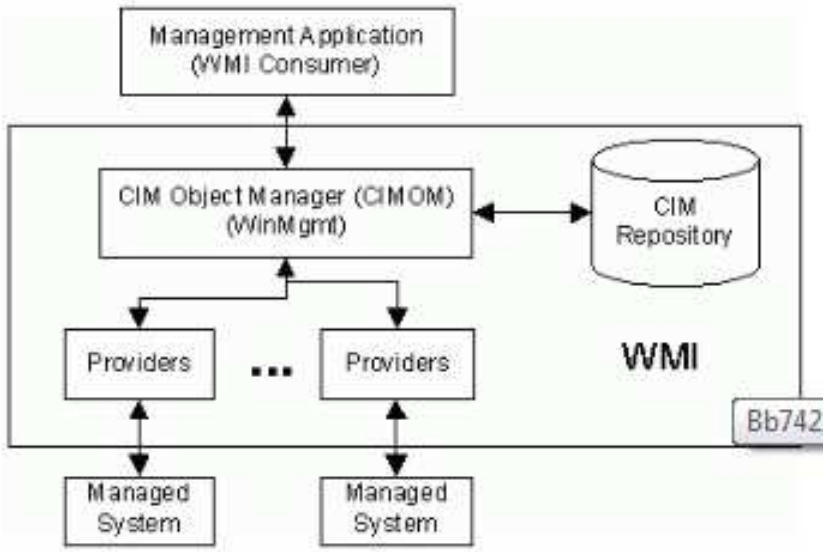
(Mauro & Schmidt 2005; Allied Telesis 2015; ManageEngine 2015.)

4.3 Windows Management Instrumentation

WMI on standardoitu hallintainfrastruktuuri ja tarkoitettu käytettäväksi laitteilla, jotka toimivat Microsoft Windows -käyttöjärjestelmällä. WMI on osa Microsoft Web-Based Enterprise Management (WBEM) -toteutus ja toimii WinMgmt-palveluna Windows-käyttöjärjestelmässä. WBEM on tekniikka, josta yritetään luoda standarditekniikka hallintatietojen käsittelemiseen yritysympäristössä. WMI perustuu avoimeen Common Information Model (CIM) -standardiin, jolla määritetään, millä tavalla laitteiden hallittavat elementit voidaan ilmentää olioina (object) ja luoda riippuvuuksia niiden välille. Jotta olioiden saamia muuttujia voitaisiin lukea tietokoneen tai ihmisen toimesta, Managed Object Format (MOF) -

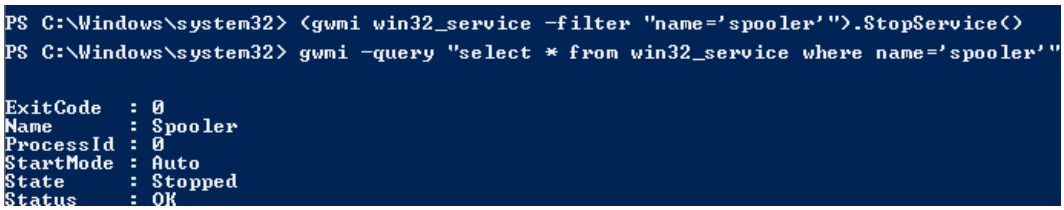
syntaksia hyödynnetään tiedon esittämisessä. WMI on yhtenäinen rajapinta, jonka kautta päästään vaikuttamaan hallittaviin olioihin ja niiden arvoihin. WMI-hallintainfrastruktuuria hyödyntäen voidaan kerätä olioista valvontatietoa, käskyttää niitä tai hallita niitä erilaisilla ohjelmilla tai komentosarjoilla. (Microsoft 2015e; Microsoft 2015g.)

WMI-arkkitehtuuri (KUVIO 13) koostuu hallintainfrastruktuurista ja WMI-välittäjistä (provider). Hallintainfrastruktuuri käsittää CIM Object Managerin ja CIM Repositoryn. CIM Object Managerin tehtävänä on toimia välikätenä hallintaohjelmille tarjoamalla pääsy CIM repositoryyn ja WMI-välittäjiin. CIM repository on keskitetty säilö hallintadatalle. WMI-välittäjien tehtävänä on toimia välikätenä hallittaviin kohteisiin. Osa WMI-välittäjistä on standardoitu ja ovat sisäänrakennettuja. Standardoituja WMI-välittäjiä ovat esimerkiksi Performance Counter-, SNMP-, Event Log- ja Win32-välittäjät. Sopivaa WMI-välittäjää hyödyntäen voidaan hakea hallittavasta kohteesta haluttu tieto. Jokainen käyttöjärjestelmässä toimiva sisäinen järjestelmä tarvitsee oman WMI-välittäjänsä, jotta järjestelmätietoihin päästäisiin käsiksi. Hallittavat kohteet voivat olla joko fyysisiä tai loogisia komponentteja yrityksessä, kuten laitteen komponentti, suuri järjestelmä, prosessi, palvelu tai ohjelma. (Microsoft 2015e; Microsoft 2015g.)



KUVIO 13. WMI-arkkitehtuuri (Microsoft 2015g.)

WMI:n pääasiallinen tarkoitus on mahdollistaa laitetietojen keruu ja laitteidenhallinta Windows-ympäristöissä. WMI on erittäin monipuolinen käyttötarkoituksiltaan, ja sitä hyödyntäen voidaan esimerkiksi valvoa järjestelmien ja palvelinten tilaa kokonaisvaltaisesti, yksittäisiä ohjelmia ja niiden prosesseja, palvelimen palveluja, Windowsin tapahtumalokia ja Windowsin suorituskykyä (performance counters). Koska WMI mahdollistaa erilaisten komentosarjojen suorittamisen, sen avulla voidaan esimerkiksi vikatilanteissa vaihtoehtoisesti käynnistää tai pysäyttää palveluja (KUVIO 14). Komentosarjat voidaan vikatilanteissa automatisoida. Oletuksena WMI-istunnot muodostetaan COM:n tai DCOM:n kautta, mutta vaihtoehtoisesti voidaan hyödyntää Windows Remote Management -palvelua. (Microsoft 2015f; Microsoft 2015g.)



KUVIO 14. Microsoft PowerShell -komentosarja WMI-kohteen hallintaan

4.4 Windows Remote Management

Windows Remote Management (WinRM) on Web Services for Management -protokollaa (WS-Management) hyödyntävä palvelimien etähallintaan tarkoitettu standardi. WS-Management-protokolla pohjautuu Simple Object Access Protocol (SOAP) -protokollaan. Järjestelmäylläpitäjät voivat WinRM-palvelua hyödyntäen etähallita Windows-palvelimia ja suorittaa niillä komentoja. WinRM käyttää tiedon hakuun Windowsissa WMI-hallintainfrastruktuuria. Oletuksena Windows-palvelimet eivät käytä WinRM-palvelua, joka prosessoi WinRM WS-management -protokollan pyyntöjä vaan se on otettava käyttöön erikseen. WinRM:n avulla on mahdollista tehdä kyselyitä myös muihin käyttöjärjestelmiin, jotka tukevat sitä kuten Linux. WinRM on monikäyttöinen, ja sitä voidaan hyödyntää hallinnan ohella valvonnassa. WinRM ja sitä tukevaa mikrokontrolleria hyödyntäen voidaan palvelimia

esimerkiksi käskyttää IPMI WMI -välittäjän kautta, vaikka palvelimet olisivat pois päältä tai vikaantuneita. (Microsoft 2015c; Microsoft 2015h.)

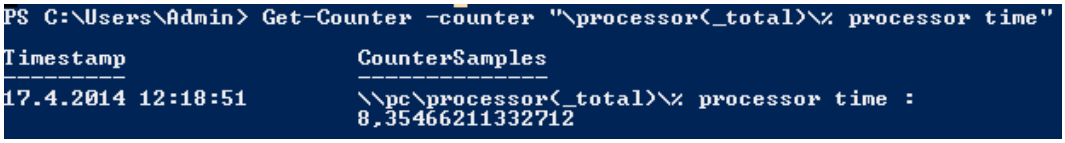
Windows Remote Shell (WinRS) on asiakasohjelma, jonka avulla voidaan käskyttää palvelimia etänä ja kerätä tietoa. Paikallisesti tietoa voidaan hakea WinRM-komennolla. WinRM-palvelu käytännössä kuuntelee etähallintakutsuja ja välittää ne eteenpäin paikallisille välittäjille, esimerkiksi Powershellille- tai WMI-välittäjille. WinRM-tekniikan suuri etu verrattaen DCOM-tekniikkaa hyödyntäviin asiakasohjelmiin on WinRM:n tapa muodostaa istunnot. WinRM muodostaa istunnot yksinkertaisesti HTTP-protokollan avulla käyttäen vain yhtä porttia. WinRM on erittäin helposti konfiguroitavissa palomuureille ja käytettävissä, koska se käyttää toiminnassaan HTTP-protokollaa ja XML-tiedostoformaattia. Tiedon salauksessa on mahdollista käyttää SSL-pohjaista salausta. (Microsoft 2015c.)

4.5 Windows Performance Counters

Windows performance counters eli Windowsin suorituskykylaskurit tarjoavat tietoa käyttöjärjestelmän, ohjelman, palvelun tai ajurin suorituskyvyn tilasta. Suorituskykylaskureita voidaan lukea Performance Counter Application Programming Interface -ohjelmointirajapintaa (API) hyödyntäen. Suorituskykylaskurit sisältävät raakaa pelkistettyä tietoa, jota yleensä tulkitaan siihen soveltuvalla ohjelmalla, kuten verkonvalvontaohjelmalla tai Windows-palvelimen omalla Performance Monitor -ohjelmalla. Suorituskykylaskurit ovat merkittävä tiedonlähde Windows-palvelinten valvonnassa, ja yleensä niitä luetaan hyödyntämällä WMI-arkkitehtuuria. (Microsoft 2015a; Microsoft 2015d.)

Suorituskykymittareista osa ovat oletuksena jo käyttöjärjestelmän asennuksessa (KUVIO 15) mukana, mutta osa suorituskykymittareista tulevat asennettavan ohjelmiston mukana. Ohjelmistojen kehittäjät voivat lisätä ohjelmiinsa omia suorituskykymittareita, jotka ovat täysin ohjelmakohtaisia. Mukautetuilla suorituskykymittareilla saadaan tarkkaa tietoa ohjelman toiminnasta ja sen ongelmakohdista. Tuotteet, kuten Citrix

XenApp ja XenDesktop, sisältävät omia mukautettuja suorituskykylaskureitaan, jotka ovat hyödynnettävissä.



KUVIO 15. Powershell-kysely Windows suorituskykylaskurin arvosta

5 CITRIX EDGESIGHT 5.4

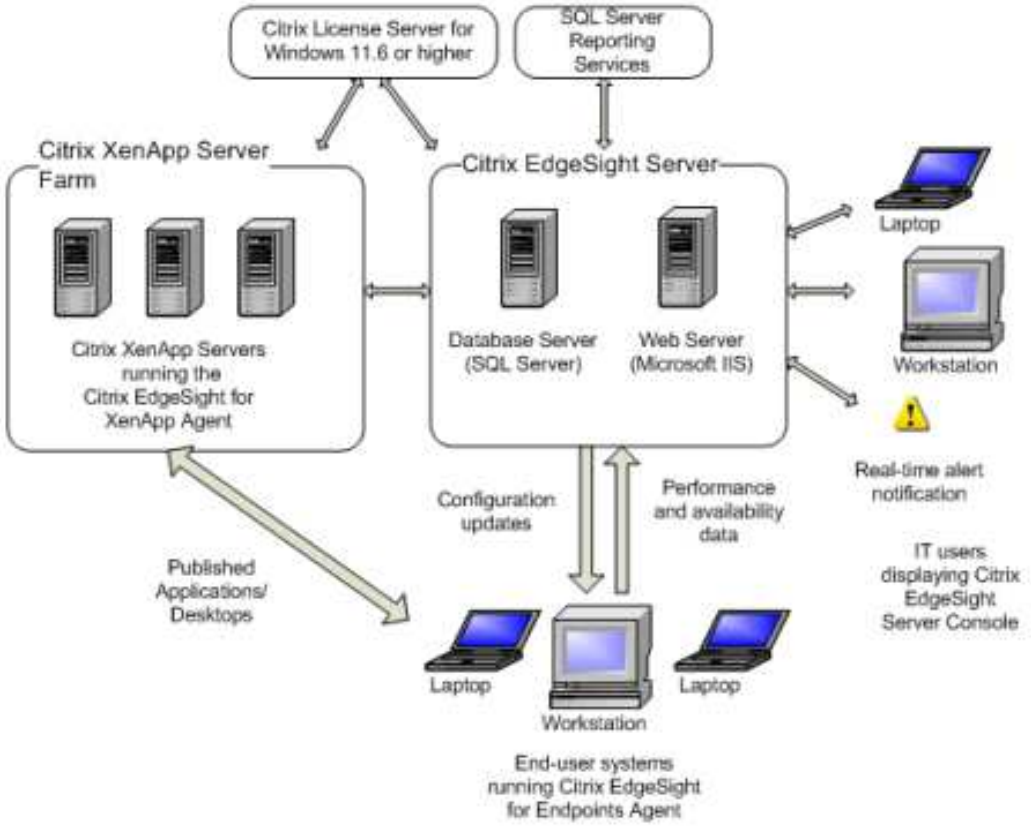
5.1 Citrix EdgeSight 5.4: Yleistä

EdgeSight on Citrixin oma Citrix-ympäristön suorituskyvyn valvontaan ja palvelujen saatavuuteen keskittyvä ratkaisu, jonka painopiste on XenApp-järjestelmässä ja sen loppukäyttäjissä. EdgeSight pystyy kuitenkin valvomaan XenDesktop-järjestelmää tietyin rajoituksin. Citrix EdgeSight on osana Citrix XenDesktop- ja XenApp-järjestelmien lisensointia. EdgeSight-valvontaratkaisu on saatavilla esimerkiksi XenDesktop platinum -lisenssin kautta. (Citrix Systems, Inc. 2015a.)

Citrix EdgeSightin vahvuudet ovat suorituskyvyn valvonnassa ja painottuvat juuri Citrixin omiin järjestelmiin ja ICA-istuntojen sekä käyttäjäkokemuksen valvontaan. EdgeSight-järjestelmällä voidaan esimerkiksi valvoa ja mitata käyttäjäkokemusta reaaliajassa ICA-istuntojen kautta, tunnistaa ja diagnosoida ongelmat kirjautumisprosesseissa, arvioida julkaistujen ohjelmien toimintaa ja diagnosoida julkaistujen ohjelmien ongelmat reaaliajassa. EdgeSight-järjestelmällä on mahdollista myös valvoa Citrix-palvelinten tilaa ja Citrix-ympäristön verkon liikennettä. Valvonnan ohella EdgeSight tarjoaa mahdollisuuden tuottaa raportteja valvontatiedoista, joita voidaan myös hyödyntää ympäristön suunnittelussa. Järjestelmän avulla voidaan myös kartoittaa tarvittavia laiteresursseja, jotta niitä olisi tarpeeksi käyttäjille vapaana myös tulevaisuudessa. Citrix EdgeSight on integroitavissa muiden verkonvalvontaohjelmien kanssa kuten Microsoft System Center Operations Managerin. (Citrix Systems, Inc. 2007.)

5.2 Citrix EdgeSight 5.4: komponentit ja arkkitehtuuri

EdgeSight-järjestelmä koostuu XenApp-ympäristössä (KUVIO 16) EdgeSight-agenteista, -palvelimesta, -palvelinkonsolista, Citrix-lisensointipalvelimesta. EdgeSight-järjestelmän kanssa voidaan hyödyntää tarvittaessa sähköpostipalvelinta ja SNMP-palvelinta. (Citrix Systems, Inc. 2010a.)



KUVIO 16. Citrix EdgeSight 5.4 -komponentit (Citrix Systems, Inc. 2010a.)

EdgeSightin valvonta perustuu EdgeSight-agenttien ja -palvelimien väliseen kommunikointiin (KUVIO 16). Agentit toimivat palvelimissa ja päätelaitteissa palveluna (rscorsvc) keräten tietoa paikallisesta ympäristöstään ja tallentamalla sen paikalliseen firebird-tietokantaansa (fbserver). Tietyin väliajoin agentit yhdistävät datansa TCP-hyötykuormaan ja lähettävät ne eteenpäin EdgeSight-palvelimelle. Agentit voivat lähettää myös hälytyksiä tarvittaessa. EdgeSight-agentit voidaan jakaa kolmeen eri tyyppiin valvottavasta kohteesta riippuen: XenApp agent, Virtual Desktop agent ja Endpoint agent. XenApp agenteista on kahta eri versiota: tavallinen (basic) ja kehittynyt (advanced), joista tavallinen versio rajoittaa valvontaa keskittyen asiakas- ja palvelinpään suorituskyvyn ja julkaistujen ohjelmien käytön mittaukseen. Kehittyneempi versio tarjoaa kaikki ominaisuudet käyttöön, esimerkiksi tarkemmat tiedot käyttäjien ICA-istunnoista ja verkkoyhteyksien valvonnan. (Citrix Systems, Inc. 2010a.)

EdgeSight-palvelin kerää tietoa EdgeSight-agenteilta ja huolehtii valvontadatan esittämisestä järjestelmän ylläpitäjille. EdgeSight-palvelin koostuu XenApp-ympäristössä kolmesta eri komponentista: web-, tietokanta- ja raportointi-palvelimesta. Web-palvelin ottaa vastaan agenttien lähettämän valvontadatan ja mahdollistaa graafisen näkymän kerätystä tiedosta palvelinkonsolin kautta. Web-palvelin hyödyntää toiminnassaan Microsoftin IIS-palvelinohjelmistoa. Tietokantapalvelin on agenteilta kerätyn valvontadatan keskitetty säilytyspaikka. Raportointipalvelimen avulla saadaan luotua raportteja ympäristön suorituskyvystä ja toiminnasta. Jos EdgeSight otetaan käyttöön myös XenDesktop-ympäristössä, tarvitaan ylimääräisiä palvelinkomponentteja mukaan. EdgeSight Agent Database Server -palvelin sisältää virtuaalityöpöytien agenttien lähettämän valvontadatan ja Agent data file share -tiedostojakoon säilötään kaikki tiedostot, joita ei voida tietokantaan tallentaa, kuten lokitiedostot. (Citrix Systems, Inc. 2010a.)

EdgeSight-palvelinkonsoli sijaitsee EdgeSight-palvelimella, johon otetaan yhteys selaimella EdgeSight-palvelimen WWW-osoitteeseen. Konsoli avataan selaimeen, jonka avulla järjestelmien ylläpitäjät ovat yhteydessä EdgeSight-palvelimeen. Palvelinkonsolin kautta voidaan esimerkiksi konfiguroida EdgeSight-palvelinta ympäristöön sopivammaksi, valvoa Citrix-ympäristöä ja luoda raportteja. Konsoli voidaan jakaa käyttötarkoituksen mukaan kuuteen eri toiminalliseen alueeseen (KUVIO 17): ympäristön valvonta (monitor), vianetsintä (troubleshoot), suunnittelu ja hallinta (plan and manage), käytön seuranta (track usage), raporttien selaus (browse) ja palvelimen asetukset (configure). (Citrix Systems, Inc. 2010a.)

KUVIO 17. Citrix EdgeSight -palvelinkonsoli näkymä

5.3 Citrix EdgeSight 5.4: peruskäsitteet

EdgeSight-palvelimen käytön kannalta on olennaista tietää peruskäsitteet ja niiden tarkoitus. Yritys (company) on EdgeSight-palvelimen ensisijainen hallinnollinen yksikkö. Palvelimelle on mahdollista lisätä useita yrityksiä. Yritykset sisältävät osastoja (departments), jotka jakautuvat hierarkisesti alaspäin valvottavien kohderyhmien mukaan: XenApp, XenDesktop ja päätelaitteet. Jokainen kohderyhmä sisältää EdgeSight-agenteilla varustetut laitteet (devices). Citrix-järjestelmiin sidotut kohderyhmät ovat oletettu lähtökohta konfiguroinnissa, mutta tarvittaessa voidaan eri järjestelmien laitteita liittää samaan ryhmään muodostamalla mukautettu ryhmä (custom group). Laiteryhmien lisäksi, voidaan myös tehdä mukautettuja käyttäjäryhmiä (user groups). (Citrix Systems, Inc. 2011a.)

EdgeSight-palvelinta hallitaan käyttäjien (users) toimesta, joilla jokaisella voi määrätä omat roolinsa (roles) työkuvansa mukaan. Järjestelmäylläpitäjä voi tehdä muutoksia kokonaisvaltaisesti, ja vaihtoehtoisesti ulkopuoliselle käyttäjälle voidaan antaa rajoitetut oikeudet vain raporttien muodostamiseen ja selaamiseen tietokannasta. Käyttäjärooleja voidaan mukauttaa käyttäjäoikeuksien kautta (user

permissions). EdgeSight mahdollistaa myös raporttitilauksien muodostamisen (subscriptions), jotka voivat olla esimerkiksi raportteja ennaltamäärättyjen palvelutasosopimusten toteutumisesta määrätyllä aikavälillä. (Citrix Systems, Inc. 2011a.)

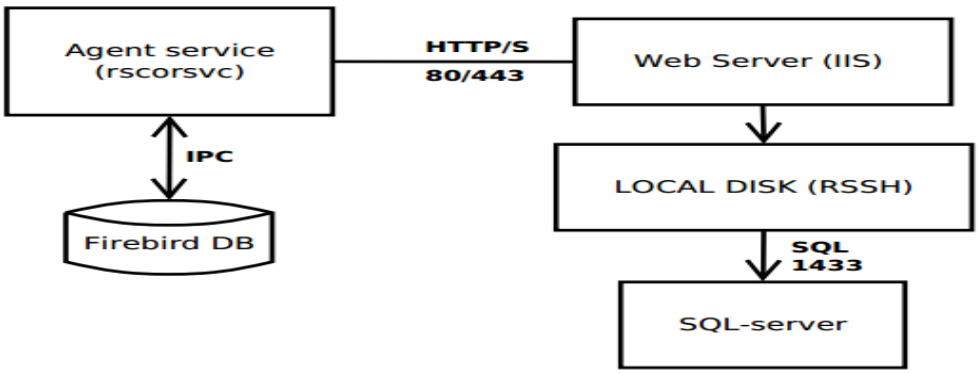
5.4 Citrix EdgeSight 5.4: valvonta

EdgeSight hyödyntää valvonnassaan Windowsin suorituskykymittareita, tapahtumalokeja, ICA-istuntoja, XenApp- ja XenDesktop-agenttien tallentamaa dataa sekä palvelimissa ja työasemissa WMI-arkkitehtuuria. EdgeSight-agenttien keräämä tieto voidaan jakaa kolmee eri kategoriaan: suorituskyky-dataan, tapahtumiin liittyvään dataan ja XenApp- sekä XenDesktop-dataan. Suorituskykyyn liittyvä data sisältää tietoja muun muassa prosessorin, muistin ja levyn käytöstä. Tapahtumiin liittyvä data sisältää julkaistujen ohjelmien virhetietoja, ohjelmien ja verkon käyttöön liittyvää tietoa. XenApp- ja XenDesktop-data sisältää paljon ICA-istuntoihin, Citrix-palveluihin, käyttäjiin, keskittyvää tietoa ja käyttäjäkokemukseen liittyvää tietoa. (Citrix Systems, Inc. 2010a.)

EdgeSight hyödyntää käyttäjäkokemuksen mittaamisessa ICA-protokollaa ja sen virtuaalikanavassa kulkevaa Citrixin End User Experience Monitoring (EUEM) -suorituskykymittareita. EUEM-mittarit tallennetaan Session Experience Monitoring Service (SEMS) -palvelua hyödyntäen laitteen muistiin, josta EUEM-mittarit julkaistaan EdgeSight-agentille ja tallennetaan Firebird-tietokantaan. (Citrix Systems, Inc. 2015c.)

Jotta valvontadataa pystyttäisiin ylipäätänsä lukea palvelimen konsolin kautta, EdgeSight-agentin on käytävä tiedonlähetysprosessi läpi (KUVIO 18). Oletuksena agentit lähettävät keräämänsä tiedon kahdesti päivässä EdgeSight-palvelimelle. Agentin tehtävänä on selvittää ensin palvelimelta, mitä tietoa lähetetään, ja palvelin lähettää vastauksen agentille, mitä tietoa tarvitaan. Palvelimen pyynnöstä riippuen, laitteen paikallisesta Firebird-tietokannasta lähetetään tietoa palvelimelle HTTP- tai HTTPS-protokollan avulla ja tallennetaan palvelimen paikalliselle levylle. EdgeSight Script Host (RSSH) -palvelu hakee ja käy läpi tiedon palvelimen levyltä. Lopuksi

RSSH lähettää valvontadatan SQL-palvelimelle lopulliseen varastointiin. Kuvion 18 prosessi kuvaa agentin perustoimintaa, mutta reaaliaikaisessa suorituskyvynvalvonnassa palvelin tekee kyselyt suoraan agenttien Firebird-tietokantaan TCP-porttiin 9035 ja tieto lähetetään suoraan palvelinkonsolin näkymään reaaliajassa. Reaaliaikaisesti valvottavaa dataa ei tallenneta EdgeSight-palvelimelle. (Citrix Systems, Inc. 2010a.)



KUVIO 18. EdgeSight-agentin valvontadatan lähetysprosessi

6 MICROSOFT SYSTEM CENTER OPERATIONS MANAGER 2012

6.1 SCOM 2012: yleistä

System Center Operations Manager 2012 (SCOM) on Microsoftin System Center -tuoteperheeseen kuuluva infrastruktuurin valvontajärjestelmä. SCOM on suunnattu kaikenkokoisille yrityksille, jotka haluavat valvoa laitteitaan, virtuaalikoneitaan, palvelujaan, käyttöjärjestelmiään, ohjelmiaan ja verkkoaan. SCOMin avulla IT-yksiköt voivat havaita ja korjata mahdolliset ongelmat ja niiden aiheuttajan ympäristössään ennen kuin niistä aiheutuu käyttäjille suuria ongelmia. (Microsoft 2013g.)

SCOM 2012 -järjestelmä hyödyntää erilaisia valvontatekniikoita ja rajapintoja valvonnassaan. SCOM hyödyntää pääasiallisesti Windows-palvelinten valvonnassa ja hallinnassa WMI-arkkitehtuuria, WinRM-tekniikkaa, suorituskykylaskureita, tapahtumalokeja ja powershell -komentokehotetta. SCOM-järjestelmällä on mahdollista valvoa laitteita, jotka tukevat SNMP- versioita 1, 2c ja 3. Järjestelmä mahdollistaa myös Javaan pohjautuvien ohjelmien, UNIX- ja Linux-palvelimien sekä Microsoftin .NET Framework -ohjelmistokomponenttikirjastoa hyödyntävien ohjelmien valvonnan. (Microsoft 2013g; Microsoft 2013f.)

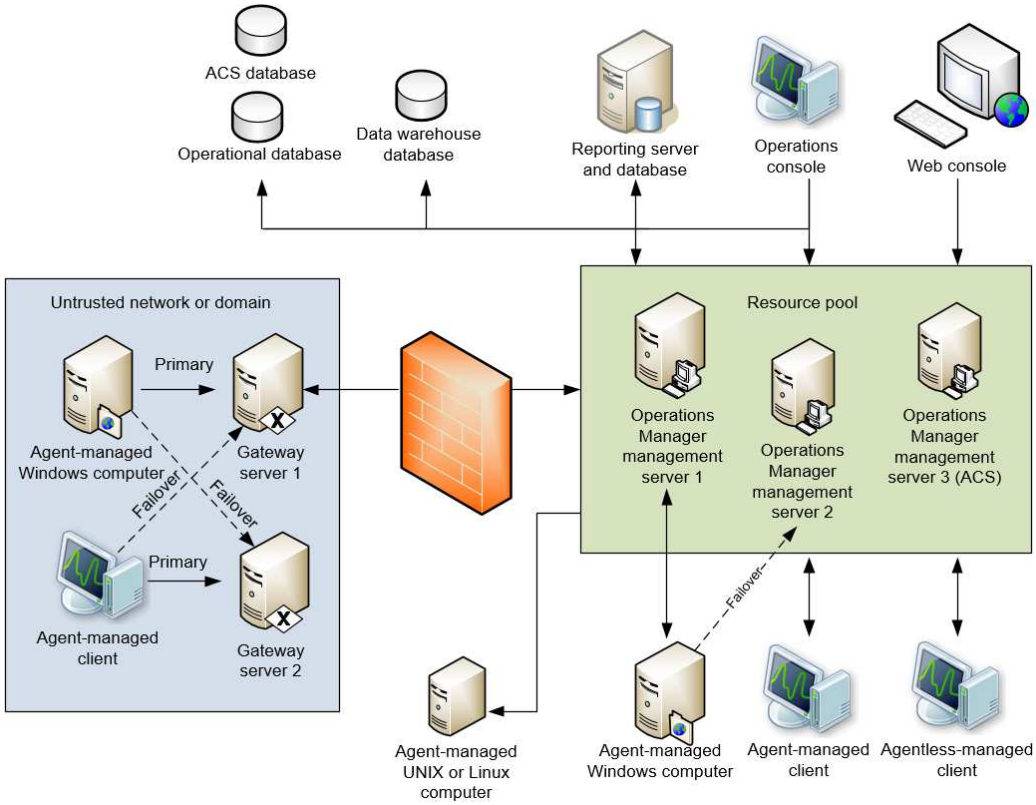
6.2 SCOM 2012: komponentit ja arkkitehtuuri

SCOM 2012 -järjestelmä koostuu hallintaryhmästä (management group), joka luodaan aina järjestelmän käyttöönoton yhteydessä. Hallintaryhmä voidaan muodostaa minimissään hallintapalvelimesta (management server), operatiivisesta tietokannasta (operational database) ja raportointi-tietokannasta (reporting data warehouse database) (KUVIO 19). Valvottaviin palvelimiin yleensä asennetaan erillinen asiakaspään valvontaohjelma (agent), mutta valvonta ilman agenttia on myös mahdollista. Valinnaisina komponentteina voidaan asentaa raportointi-palvelin (reporting server). Kaikki hallintaryhmän komponentit voidaan asentaa samalle palvelimelle tai hajauttaa suuremmissa ympäristöissä omille palvelimille. SCOM 2012 tarvitsee toimiakseen myös toimintaansa

tukevia järjestelmiä, kuten Active Directorya ja Domain Name Services -palvelinta. (Microsoft 2013g.)

KUVIO 19. SCOM 2012 -komponentit (Microsoft 2013g.)

Hallintapalvelin toimii koko SCOM-järjestelmän keskipisteenä. Hallintapalvelimen tehtävänä on toteuttaa tehdyt muutokset hallintaryhmään, hallita ja viestiä laitteiden agenttien kanssa sekä päivittää hallintaryhmän tietokantoja ajantasalle. SCOM-järjestelmää ylläpidetään ja valvotaan hallintakonsolilla (operations console) tai selaimen kautta web-konsolilla (web console). Kun hallintaryhmään lisätään useampi kuin yksi hallintapalvelin, muodostetaan hallintapalvelimista oma ryhmä (resource pool) (KUVIO 20). Ryhmässä olevat hallintapalvelimet kommunikoivat toistensa kanssa automaattisesti ja huolehtivat vikasietoisuudesta sekä kuormanjaosta. Jos laitteita halutaan valvoa internetin yli epäluotettavista verkoista tai AD-toimialueilta (KUVIO 20), voidaan hallintapalvelinten rooli tarvittaessa muuttaa yhdyskäytävä-palvelimeksi luottamattomien domainien välille. (Microsoft 2013g.)



KUVIO 20. SCOM 2012 -arkkitehtuuri (Microsoft 2013f.)

SCOM-järjestelmän operatiivinen- ja raportointi-tietokanta sijaitsevat SQL-palvelimella. Operatiivisessa tietokannassa säilytetään konfigurointidataa hallintaryhmästä ja säilytetään laitteilta saatua valvontadataa lyhytaikaisesti. Valvontadataa säilytetään oletuksena viikon ajan. Raportointi-tietokannassa säilytetään valvonta- ja hälytysdataa, jota voidaan pitkäaikaisesti hyödyntää historiallisessa raportoinnissa. Raportti-tietokantaan tallennetaan myös lyhytaikaista valvonta- ja hälytystietoa. Raportointi-tietokannan hyödyntämiseen tarvitaan erillistä raportointi-palvelinta, jonka avulla voidaan rakentaa ja esittää raportteja. (Microsoft 2013g.)

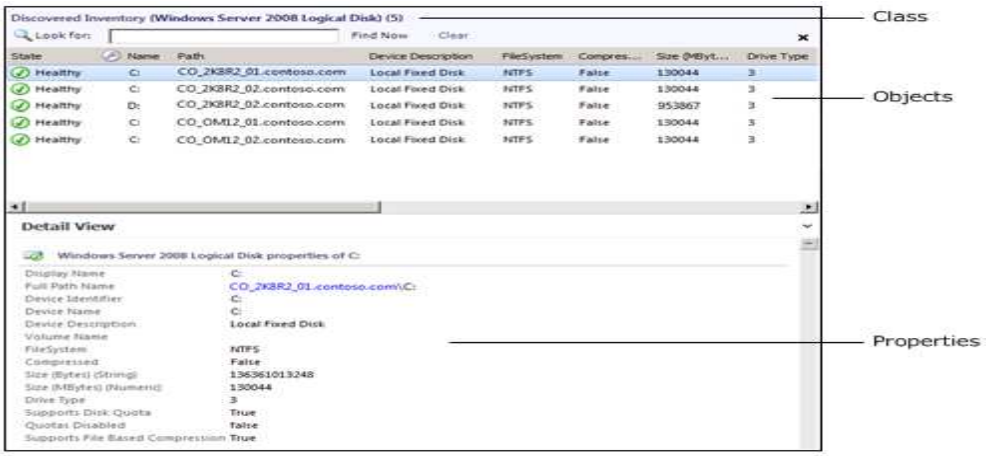
Valvottavien laitteiden agentit ovat tietokoneille asennettuja ohjelmia, jotka toimivat tietokoneessa HealthService-palveluna. Agentit raportoivat oman hallintaryhmänsä hallintapalvelimen kanssa. Agenttien tehtävänä on kerätä tietokoneesta tietoa ja verrata sitä määritettyihin arvoihin. Agentit luovat hälytyksiä tarvittaessa, jos määritetyt arvot poikkeavat viitearvoista. Agenteilla voidaan myös suorittaa tietokoneilla erilaisia toimintoja

vikatilanteiden selvittämiseksi. Proxy-agenteilla on mahdollista välittää valvontatietoa laitteista, joihin ei ole mahdollista asentaa omaa agenttia kuten loogisiin kokonaisuuksiin esimerkiksi klustereihin. Proxy-agentteja käytetäänkin hyödyksi kaikissa suurissa kokonaisuuksissa, jotka ovat yleensä myös yrityksen kriittisimpiä palveluja. (Microsoft 2013g.)

Tukijärjestelmien rooli SCOM-järjestelmän toiminnassa on keskeinen. Active Directoryn avulla SCOM-järjestelmälle voidaan toteuttaa tietoturva-asetuksia, pääsynhallintaa, tunnistautumista ja valtuuttamista. Active Directorya voidaan hyödyntää myös agenttien asetustietojen jakamiseen ja tallentamiseen. Active Directoryn toimintaa tukien nimipalvelu pitää olla asennettuna ja toiminnassa. (Microsoft 2013i.)

6.3 SCOM 2012: peruskäsitteet

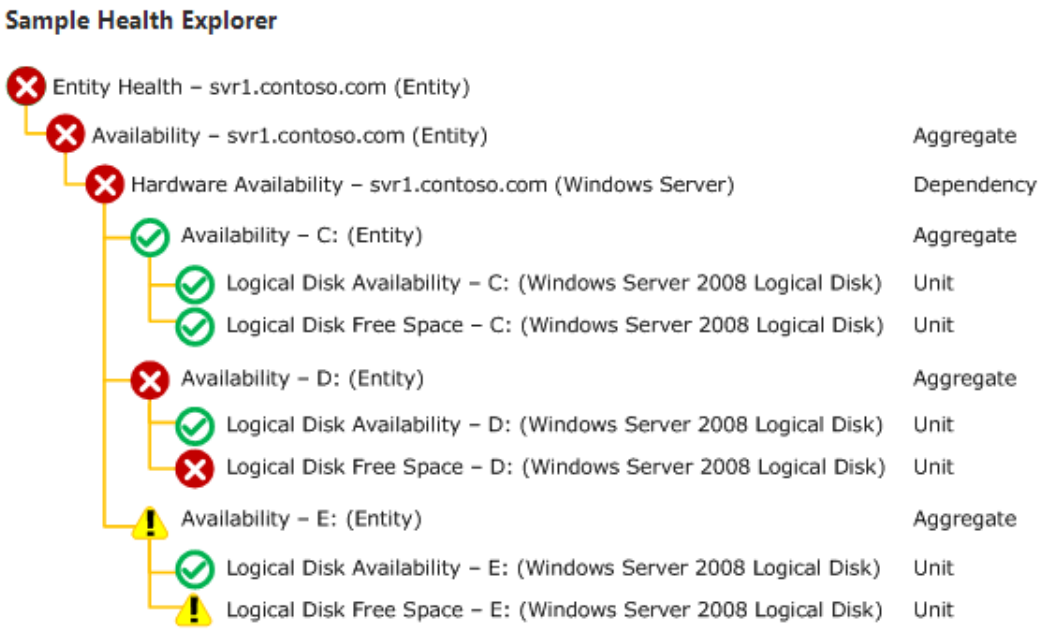
SCOM 2012 -järjestelmän käyttöä ja ymmärtämistä helpottavat yleisten termien sisäistäminen. SCOM 2012 -järjestelmän perusyksikkönä toimii kohde (object) (KUVIO 21). Kohteiksi voidaan mieltää esimerkiksi tietokone, kovalevy, tietokanta tai yrityksen AD-toimialue. Kohteet voidaan mieltää luokkien (class) instansseina. Saman luokan sisällä olevilla instansseilla on samat ominaisuudet, mutta kohteiden ominaisuuksilla on omat arvonsa. Jotta kohteita ylipäätänsä voitaisiin tarkastella SCOMin avulla, kohteet täytyy saada selville (discovery) ja lisätä järjestelmään. (Microsoft 2013j.)



KUVIO 21. SCOM 2012 luokka, kohteet ja ominaisuudet (Microsoft 2013j.)

Valvojat (monitors) ja säännöt (rules) mittaavat ja tarkkailevat valvottavien kohteidensa tilaa. Valvojat keskittyvät vain ja ainoastaan valvomaan kohteen tilaa yleisesti ja ne voivat saada kolme eri tilaa: Healthy, Warning ja Critical. Jokaiselle tilalle voidaan määrittää omat raja-arvot. Tilat määräytyvät hierarkisesti kohteen tilan mukaan alhaalta ylöspäin (KUVIO 22). Valvojia voi olla kolmea eri tyyppiä: unit monitor, aggregate monitor ja dependency monitor.

Unit monitor -valvoja on yleisin, ja sen tehtävänä on esimerkiksi valvoa Windowsin suorituskykymittareita, suorittaa komentosarjaa tai tarkkailla jotain tiettyä tapahtumaa. Unit monitor -valvojilla voidaan testata tietyn ohjelman ominaisuuksia ja valvoa ongelmien esiintymistä. Aggregate monitor -valvojat valvovat samanlaisia asioita kuten kuvion 22 mukaisesti loogisten levyjen tiloja ja raportoivat kokonaisuudesta. Dependency monitor -valvojan avulla voidaan valvottavan kohteen tila sitoa täysin toisen kohteen tilaan, joka sijaitsee aivan eri luokassa. Kun kokonaisuuksista raportoidaan tilan muutoksella, käytännöillä voidaan vaikuttaa kokonaistilan käyttäytymiseen (KUVIO 22). Tilan muutos aggregate monitor -valvojaa käytettäessä voidaan toteuttaa pahimman tilan (worst state policy) mukaan tai parhaimman tilan mukaan (health state policy). Jos worst state -käytäntöä hyödynnetään, yksi kriittinen virhe unit monitor -valvojassa riittää muuttamaan kokonaistilan kriittiseksi. Best state -käytäntöä käytettäessä yksikin toimiva unit monitor- valvoja riittää pitämään tilan healthy-tilassa. Dependency monitor -valvoja tuo vielä yhden käytännön lisää, prosentuaalisen tilan muutoksen (percentage health policy). Käytäntö hyödyntää tilan muutoksessa myös worst state -käytäntöä. Tietty määritetty prosentuaalinen määrä kriittisisessä tilassa olevia valvojia aiheuttaa dependency monitor -valvojan tilan muutoksen. Kuviossa 22 käytetään worst state -käytäntöä. (Microsoft 2013b; Microsoft 2013e.)



KUVIO 22. Windows Server -luokan tila (Microsoft 2013e.)

Säännöt vastaavasti muodostavat hälytyksiä ja keräävät tietoa analysointiin ja raportointiin. Verrattuna valvojiin, säännöt eivät muuta kohteen tilaa. Sääntöjä on kolmea eri tyyppiä, ja ne voidaan luokitella toiminsa mukaan kolmeen tyyppiin: alerting rules, collection rules ja command rules. Alerting-säännöillä voidaan muodostaa hälytyksiä. Collection-säännöillä kerätään tapahtuma- tai suorituskykytietoa tietokantoihin. Command-sääntöjä käytetään komentosarjojen ajamiseen tai ajastettujen toimintojen suorittamiseen. Collection- ja command-säännöillä ei voida luoda hälytyksiä. Sääntöjä tai valvojia luotaessa, täytyy ne aina kohdistaa (target) johonkin. Jos SCOM-järjestelmään on asennettu valmiiksi joitain hallintapaketteja (management pack), kohdistetaan valvoja tai sääntö koskemaan niiden luomia luokkia, esimerkiksi Microsoft Windows Computer- tai Logical Disk (server) -luokka. Uusia kohteita voidaan luoda itse tarvittaessa, jos niitä ei ole valmiiksi olemassa. (Microsoft 2013e; Microsoft 2013h.)

SCOM-järjestelmän toiminta perustuu laajalti hallintapakettien (management pack) hyödyntämiseen valvonnassa. Hallintapaketit sisältävät eri ohjelmien tai palveluiden valvonta-asetuksia ja määrittävät, mitä tietoa agentit keräävät ja lähettävät hallintapalvelimelle.

Hallintapaketteja on kahta eri tyyppiä: avonaisia .xml- ja suljettuja .mp-tyyppisiä. Hallintapakettien tyyppi määrittää, onko sen sisältö muokattavissa. Jos suljettujen hallintapakettien sisältöön halutaan vaikuttaa, erillinen kustomoitu hallintapaketti voidaan luoda syrjäyttämään alkuperäisen hallintapaketin asetukset override-toiminnolla. Hallintapaketit koostuvat seuraavista osista: monitors, rules, tasks, knowledge, views, reports, object discoveries ja run as profiles. Hallintapaketteja löytyy monista suosituista ohjelmista ja järjestelmistä, kuten AD:stä, Citrix XenApp:sta ja XenDesktop:sta, App-V:stä, SQL-palvelimesta ja Windows-käyttöjärjestelmästä. (Microsoft 2013g; Microsoft 2013l.)

Hallintapakettien sisältämillä näkymillä voidaan käyttäjän käyttöliittymä muokata valvottavan järjestelmän mukaiseksi. Näkymät voivat olla muokattuja tai vakioituja näkymiä kohteiden tilasta ja suorituskyvystä sekä hälytyksistä. Hallintapaketit ja hälytykset sisältävät oheistietoa, joka voidaan mieltää valvojien ja sääntöjen sisältämäksi oheistiedoksi. Oheistiedon avulla voidaan esimerkiksi löytää vian lähde ja saada ohjeet sen korjaamiseen. Hallintapaketit sisältävät myös tehtäviä, jotka ovat komentosarjoja tai erillisiä ohjelmia. Tehtävillä voidaan esimerkiksi käynnistää ohjelmia ja palveluja uudelleen tai tuhota jopa tiedostoja. Tehtävät ovat sidoksissa aina omaan luokkaansa. (Microsoft 2013l; Microsoft 2013k.)

Hallintapaketin sisältämät kohteen etsintään liittyvät säännöt mahdollistavat niiden ilmentymisen valvontajärjestelmässä. Kohteita voidaan etsiä esimerkiksi rekisteriä, WMI-hallintainfrastruktuuria, komentosarjoja tai AD:ta hyödyntämällä. Jotta SCOM-järjestelmällä pystyttäisiin suorittamaan valvontaa ja hallintaa etänä, agentit ja laitteet tarvitsevat valtuutuksen. Oletuksena SCOM-järjestelmä käyttää valtuutukseen omaa default action account -käyttäjätiliä. Jos default action account -käyttäjätilillä ei ole oikeuksia valvottavaan kohteeseensa, run as profile -profiilia voidaan hyödyntää. Profiileihin voidaan liittää useita eri run as account -käyttäjätilejä, joita voidaan käyttää erillisten kohteiden valvontaan tai hallintaan. Mukauttamalla käyttäjätilejä sopiviksi tarkoitukseensa, tietoturvaa voidaan parantaa huomattavasti SCOM-

järjestelmässä. Profiileja voi olla useita hallintapaketeissa mukana. (Microsoft 2013d; Microsoft 2013l.)

6.4 SCOM 2012: toiminta ja hallinta

SCOM 2012 toiminta perustuu agenttien ja hallintapalvelimen väliseen kommunikointiin. Toiminta voidaan jakaa yleisesti kolmeen eri vaiheeseen (KUVIO 23):

1. kohteen etsiminen ja agentin asennus **(1, 2, 3)**
2. asetustietojen **(4)** pyyntö ja lähetys sekä valvontalogiikan **(6)** lähetys
3. valvontadatan lähetys ja vastaanotto **(7)**.

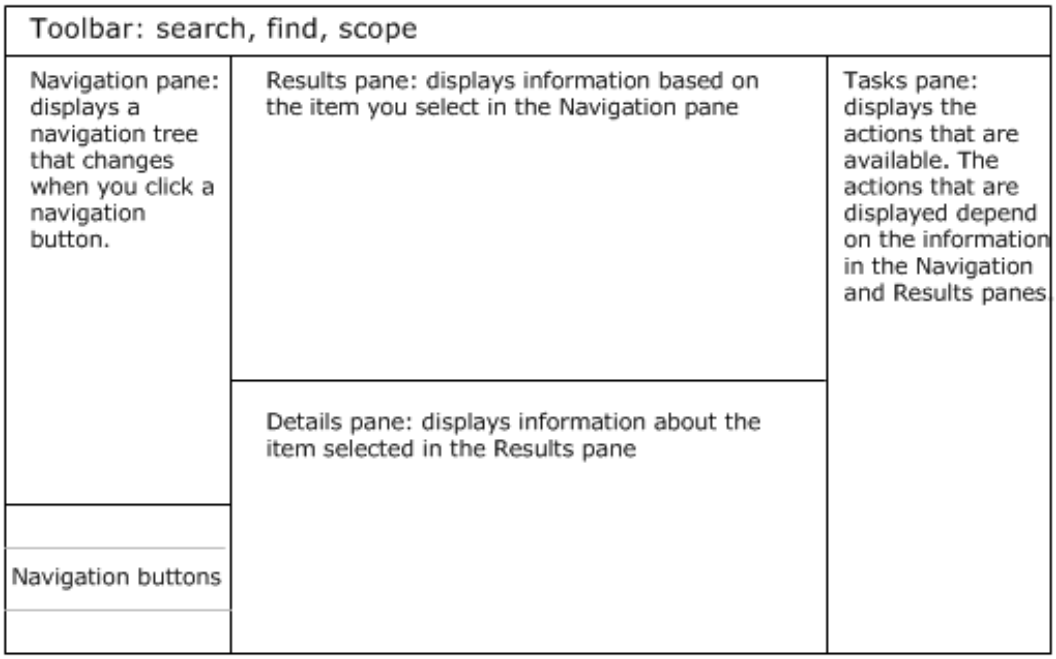
KUVIO 23. SCOM 2012:n valvonta ja toiminta (Microsoft 2013g.)

Järjestelmäylläpitäjän on löydettävä valvottavat palvelimet ensin hallintapakettia hyödyntäen. Palvelimet, jotka vastaavat hallintapaketissa määritettyjä kriteereitä, tunnistetaan. Tunnistettuihin kohteisiin voidaan asentaa valvonta-agentit joko operations console -hallintakonsolilla tai paikallisesti palvelimessa. Agentti vertaa hallintapaketin sisältämiä asetuksia palvelimeen, jolloin palvelimista saadaan esille hallintapaketissa

määritetyt luokat. Luokkien jälkeen selvitetään niiden sisältämät instanssit. Lopuksi hallintapalvelin lähettää agenteille hallintapaketin sisältämät valvojat ja säännöt, joita hyödyntämällä agentti kerää halutun tiedon ja lähettää sen takaisin hallintapalvelimelle. Jos luokkien instansseissa tapahtuu muutoksia, valvontalogiikka päivitetään uudelleen. (Microsoft 2013g.)

Kun agentit ovat asennettuina ja toiminnassa, ne lähettävät omalle hallintapalvelimelleen jatkuvasti tietoa, joka tallennetaan suoraan operatiiviseen- ja raportointi-tietokantaan. Agenttien lähettämä tieto nojautuu täysin hallintapaketin määrittämiin asetuksiin. Agenttien tiedon lähettämisen määrää pyritään rajoittamaan ja samalla pienentämään vaikutusta verkkoon ja tietokantoihin käyttämällä toleranssirajoja. Jos lähetetty arvo ei esimerkiksi poikkea yli 10 % alkuperäisestä, tietoa ei lähetetä eteenpäin. Agentit lähettävät myös omasta toiminnastaan tietoa, heartbeat-paketteja, jotka lähetetään hallintapalvelimille oletuksena 60 sekunnin välein. Jos agentti epäonnistuu neljä kertaa pakettien lähetyksessä, hälytys HealthService-palvelusta luodaan. Hälytyksen jälkeen hallintapalvelin yrittää tiedustella agentin palvelimen tilaa ICMP-ping-viestillä. Jos ping-viesti ei onnistu, luodaan hälytys palvelimen saatavuudesta. (Microsoft 2013C; Microsoft 2013g.)

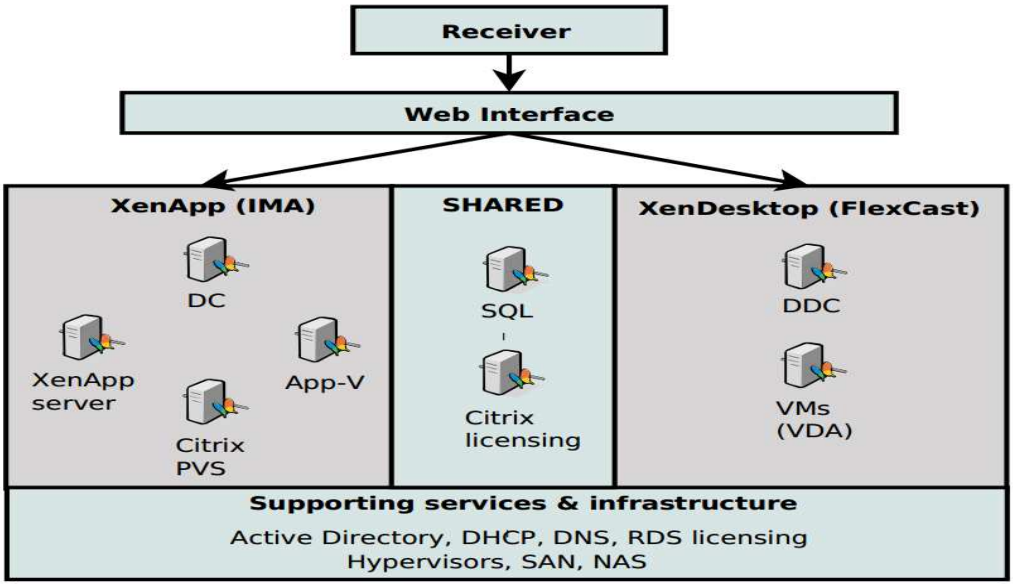
SCOM 2012 -järjestelmän määrityksiin, hallintaan ja valvontadatan tutkimiseen käytetään Operations Console -hallintakonsolia, jolla on mahdollista toteuttaa kaikki käyttäjäroolin mahdollistavat toiminnot. Selainpohjaista hallintakonsolia on myös mahdollista käyttää, mutta se rajaa käyttäjän toiminnot ainoastaan omaan työtilaan (My Workspace) ja valvontatyötilaan (Monitoring). Molemmat hallintakonsolit käyttävät kuvion 24 mukaista käyttöliittymäpohjaa. (Microsoft 2013a.)



KUVIO 24. SCOM 2012 -hallintakonsolin käyttöliittymä (Microsoft 2013a.)

7 CITRIX-JULKAISUJÄRJESTELMÄN VALVONTA

Valvonnan suunnittelun ja toteutuksen lähtökohtana oli tarkastella kahden eri valvontajärjestelmän hyödyntämistä Citrix-julkaisujärjestelmän valvonnassa. Citrixin oma EdgeSight-valvontaratkaisu on vahvimmillaan valvottaessa omia Citrix-tuotteita (KUVIO 25): Citrix XenApp, Citrix Provisioning Services, Citrix Licensing ja Citrix XenDesktop. EdgeSightin vahvuudet ovat juurikin ICA-istunnoista saatavan informaation analysoinnissa ja Citrix-palveluiden saatavuuden valvonnassa. EdgeSightin avulla on mahdollista tarkastella käyttäjän luomaa ICA-istuntoa kattavasti ja kartoittaa mahdolliset ongelmakohdat. Koska Citrix- julkaisujärjestelmä tukeutuu toiminnassaan muihin järjestelmiin, kaikkien järjestelmien toimintaa on kuitenkin valvottava yhtälailla kuin Citrix-järjestelmiäkin. Microsoft SCOM 2012:n vahvuudet ovat kokonaisvaltaisessa infrastruktuurin valvonnassa, jota voidaan helposti laajentaa tarvittaessa hallintapaketein. Microsoft SCOM 2012 mahdollistaa EdgeSightiin verrattaen hyvän automatisoinnin, hallittavuuden ja paremman vikojen diagnosoinnin sekä se skaalautuu helposti myös muille järjestelmien valvontaan. SCOM 2012 käytännössä valvoo kaikkia muita järjestelmiä (KUVIO 25).



KUVIO 25. Citrix-julkaisujärjestelmän komponentit

Molemmilla valvontajärjestelmillä on toisiinsa nähden vahvuuksia, joita hyödyntäen saadaan paikattua toistensa heikkouksia (TAULUKKO 1). Koska järjestelmiä on kaksi käytössä valvonnassa, valvonta keskitetään SCOM 2012 -valvontajärjestelmän alle, jolloin pystytään huomaamaan ja reagoimaan hälytyksiin tehokkaammin. Valvonnan keskittämisen mahdollistaa SCOM 2012- ja EdgeSight-järjestelmien keskinäinen tuki, jota hyödyntäen ne voidaan integroida toisiinsa ja EdgeSight-hälytysviestit välittää SCOM 2012 -järjestelmälle.

TAULUKKO 1. Valvontajärjestelmien vertailu

SCOM 2012 R2	**Citrix EdgeSight 5.4**
Yrityksen infrastruktuurin kokonais-valtainen valvonta	Citrix-ympäristön valvonta
Palvelimet, palvelut, tapahtumat, suorituskyky, ohjelmat, verkko, käyttöjärjestelmät	Citrix-palvelimet, ICA-istunnot, Citrix virtualisoidut työpöydät ja ohjelmat
Laajennettavuus hallintapaketeilla	Ei laajennattavissa
Suorituskyvyn- ja palvelutasonvalvonta, palvelujen saatavuus, hallittavuus, automati-sointi, raportointi, vikadiagnostiikka	Suorituskyvyn valvonta, palvelujen saatavuus, raportointi, vikadiagnos-tiikka
Helposti skaalattavissa	-
Agent/Ei agenttia	Agent
WMI, SNMP, PowerShell, komen-tosarjat	WMI, SNMP

Citrix-julkaisujärjestelmän valvonta voidaan jakaa viiteen suurempaan kategoriaan, jolloin pystytään helpommin käsittelemään kokonaisuuksia ja vastuualueita:

1. Infrastruktuuri:

- Verkko (Network)
- Laitteisto (Hardware)

2. Suorituskyky:

- Suorituskykymittarit (Performance Counters)

3. Tapahtumat:

- Käyttöjärjestelmän lokit (Windows Event Log)

4. Palvelut:

- Windows-palvelut (Windows Services)
- XenDesktop-palvelut (XenDesktop Services)
- Provisioning-palvelut (Provisioning Services)
- Lisenssi-palvelut (Licensing Services)
- Web-rajapinnan -palvelut (Web Interface services)

5. Palveluiden saatavuus

Hyödyntäen juuri molempia valvontajärjestelmiä voidaan kaikkia viittä vastuualuetta valvoa tehokkaasti. Citrix on julkaissut suosituksen Microsoft SCOM Operations Manager -valvontajärjestelmälle Citrixin valvontaan, jota voidaan käyttää soveltaen omien järjestelmien ja palveluiden tarpeeseen (liitetiedosto Operations Guide – Monitoring.pdf).

7.1 SCOM 2012 R2 –testiympäristön valmistelu

SCOM 2012 R2 asennuksen lähtökohtana oli tehdä väliaikainen testiympäristö, jossa Citrix-julkaisujärjestelmän valvontaan liittyviä asioita voitaisiin testata puuttumatta tuotannollisiin asioihin. SCOM 2012 R2 tarvitsee muutakin infrastruktuuria alleen toimiakseen kuin itsensä. Vähintäänkin asennettuina ja määritettyinä järjestelminä pitää olla Active Directory Domain Services, DNS-palvelimen ja SQL-palvelin. Yrityksessä hyödynnettiin jo olemassaolevaa yrityksen infrastruktuuria ja kotona omaa luotua virtualisoitua testiympäristöä. Yrityksestä löytyi jo asennettuna Citrix EdgeSight-palvelimen, joka oli määritelty käyttöön ja valvomassa jo

tuotannollisia asioita. Kotona olevassa sen hyödyntäminen lisenssiasioiden takia ei ollut mahdollista.

Kotona olevassa testiympäristössä hyödynnettiin Linux-käyttöjärjestelmällä toimivaa Oracle Virtualbox -hypervisoria. Linux-käyttöjärjestelmällä pyörivää virtualisoitua testiympäristöä varten asennettiin ja määriteltiin Windows Server 2012 R2 -käyttöjärjestelmällä olevat AD- (liite 2), DNS- (liite2), SQL- (liite 3) ja SCOM-palvelimet (liite 4). Testiympäristössä pyrittiin mahdollisimman yksinkertaiseen toteutukseen, jotta mahdolliset virheet saataisiin minimoitua. SCOM 2012 R2 -järjestelmän asennuksessa noudatettiin myös samaa periaatetta. Järjestelmän asennuksessa noudatettiin yhden palvelimen periaatetta ja kaikki SCOM 2012 -komponentit asennettiin samalle palvelimelle. Testiympäristö sisälsi useita palveluja, mutta ne keskitettiin kahteen järeämpään virtuaalipalvelimeen seuraavasti: SCOM 2012- ja SQL-palvelin sekä AD- ja DNS-palvelin.

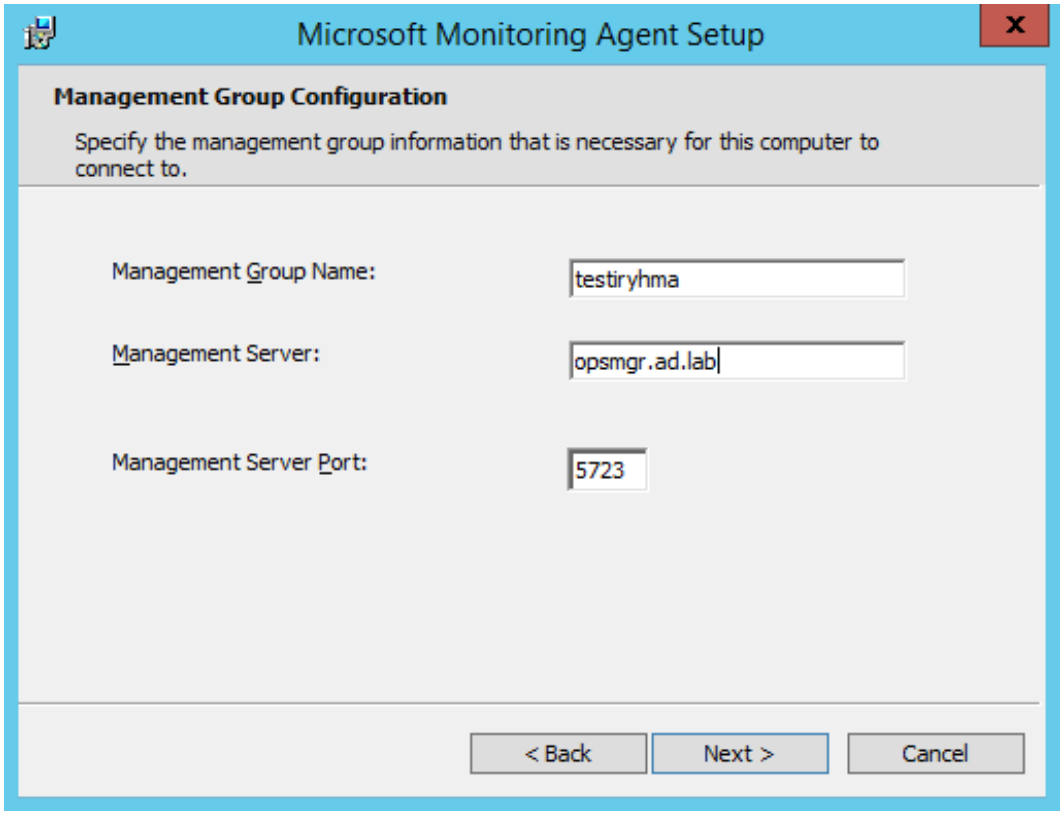
SCOM 2012 R2 vaatii asentuakseen tietyt roolit ja toiminnot: Microsoft .NET Framework 4.5., PowerShell 3.0, Report Viewer controls ja Web Server (IIS) (liite 1). Report Viewer 2012 Runtime ladataan Microsoftin sivuilta ja asennetaan SCOM-palvelimelle. Kun kaikki vaadittavat roolit ja toiminnot, Active Directory Domain Services, Microsoft SQL Server 2012 on asennettuna voidaan aloittaa SCOM 2012 R2:n asennus. SCOM 2012 R2:n asennusta aloittaessa on hyvä myös huomioitava sen vaatimat suositukset. Olisi suotavaa käyttää yhden palvelimen periaatteella virtuaalikoneella kahta ydintä tai enemmän ja kahdeksaa gigatavua muistia.

7.2 SCOM 2012 R2: valvonta-agenttien asennus ja määrittely

Yrityksen ympäristössä oli jo valmiiksi asennettuna EdgeSight ja siihen liittyvät agentit palvelimille, joten seuraavaksi tarkoituksena oli mahdollistaa valvottavien kohteiden ja SCOM 2012 R2 -valvontapalvelimen välinen kommunikointi. Tuotannollisessa ympäristössä, jossa palvelimet esimerkiksi streamataan suoraan tietystä levykuvasta suoraan, SCOM 2012- ja Edgesight -agentit voidaan asentaa

suoraan virtuaalikoneen peruslevykuvaan. Silloin niitä ei tarvitse uuden palvelimen käyttöönotossa aina asentaa uudelleen ja näin säästetään aikaa. Myös päivitykset voidaan hoitaa kätevästi päivittämällä peruslevykuvassa oleva ohjelma. Testiympäristössä Microsoft Monitoring agentti asennetaan manuaalisesti SCOM 2012 R2 mukana tulevalta medialta valvottaviin kohteisiin. Seuraavassa asennus tehtiin AD-palvelimelle. Käynnistetään Microsoft Monitoring agentin asennusohjelma ja määritellään asennuspolku.

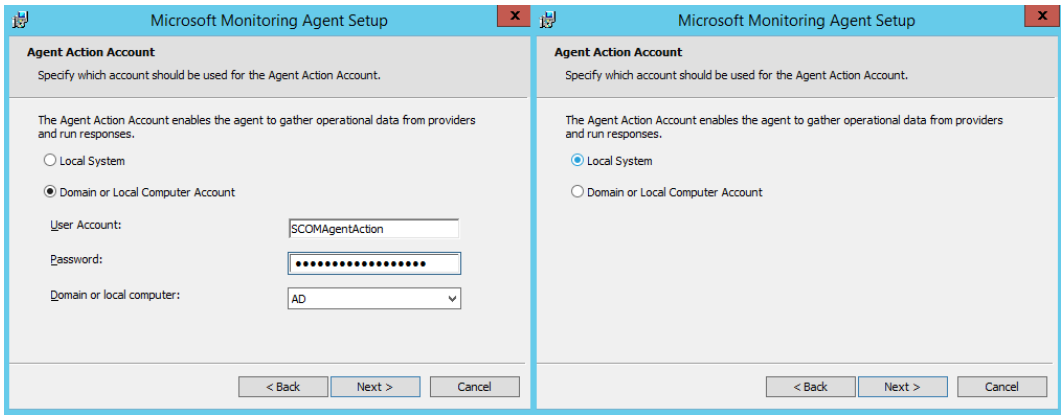
Yhdistetään seuraavaksi Microsoft Monitoring Agent SCOM 2012 R2 palvelimelle ja agentille määritetään hallintaryhmän nimi, hallintapalvelimen nimi sekä hallintapalvelimen portti (KUVIO 26) Porttina käytetään oletus-porttia.



KUVIO 26. Microsoft Monitoring Agentin hallintaryhmä, -palvelin ja -portti

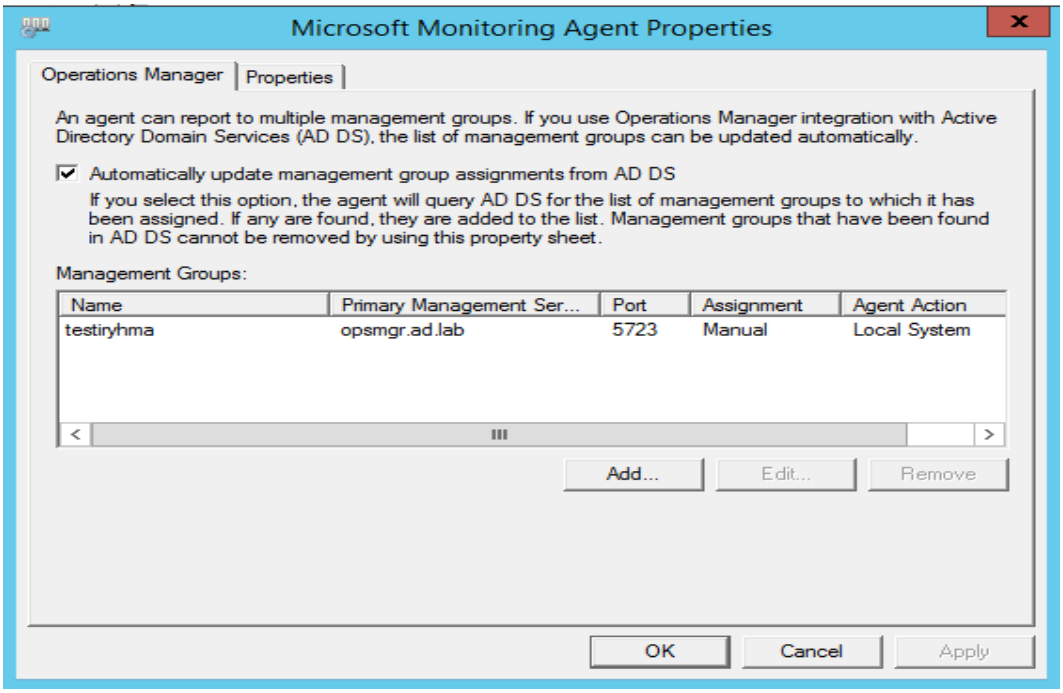
Seuraavaksi määritetään käyttäjätunnus, jota agentti käyttää valvontaan, tiedon keruuseen sekä erinäisten komentosarjojen suorittamiseen. Käytetään agentille testiympäristössä paikallisen virtuaalikoneen omaa

tunnusta (local system) (KUVIO 27), jonka jälkeen viimeistellään asennus. Vaihtoehtoisesti agentille voitaisiin käyttää esimerkiksi sille luotua domain tunnusta. Siinä tapauksessa pitäisi huomioida riittävät oikeudet agentille.



KUVIO 27. Microsoft Monitoring Agentin käytettävät tunnukset

Kun agentti on onnistuneesti asennettuna valvottavaan kohteeseen, sen asetuksia voidaan myöhemmin tarkastella tai muuttaa Windowsin hallintapaneelista kohdasta Microsoft Monitoring Agent (KUVIO 28). Agentti on nyt valmiina omalta osaltaan kommunikoimaan palvelimen kanssa.



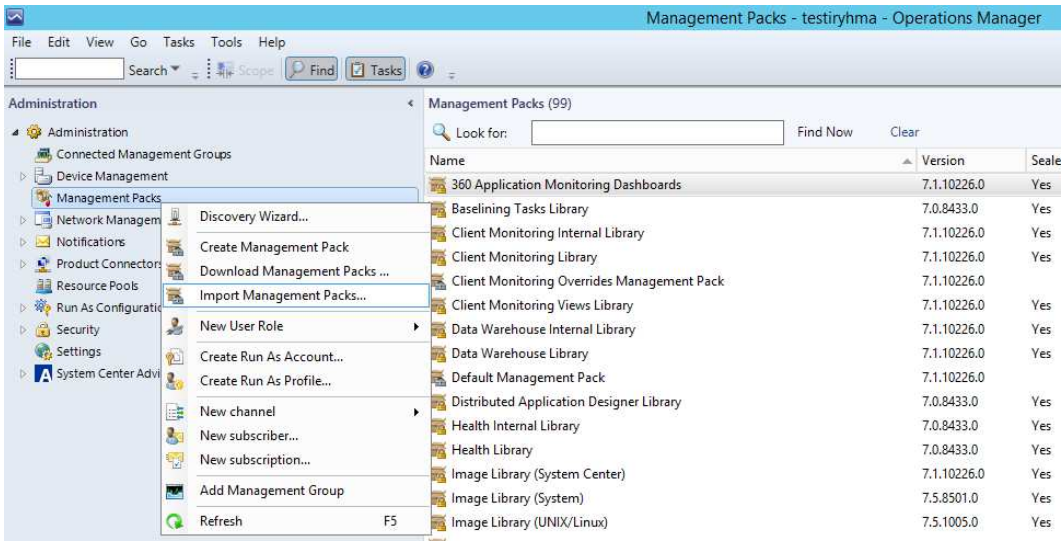
KUVIO 28. Microsoft Monitoring Agent: määritetyt asetukset

7.3 SCOM 2012 R2: hallintapakettien asennus ja kohteen lisäys

Citrix-julkaisujärjestelmän ollessa laaja ympäristö pitäen sisällään erilaisia järjestelmiä ja komponentteja asennetaan jokaista järjestelmää koskeva hallintapaketti palvelimelle. Hallintapalvelimelle asennetaan hallintapaketit yksitellen sen mukaan, mitä halutaan valvoa. Hallintapaketit asennetaan yksitellen rauhassa analysoiden niiden tuottamia hälytyksiä ja dataa, jolloin voidaan välttyä liian suurelta tiedon määrältä alkuun ja sivuuttaa mahdolliset turhat hälytykset pois (overrides). Hallintapakettien asennusvälinä olisi hyvä pitää vähintäänkin muutama päivä suuremmassa ympäristössä, jolloin saadaan varmasti vääriä hälytyksiä karsittua pois ja kartoittaa samalla oman ympäristön suorituskykyä.

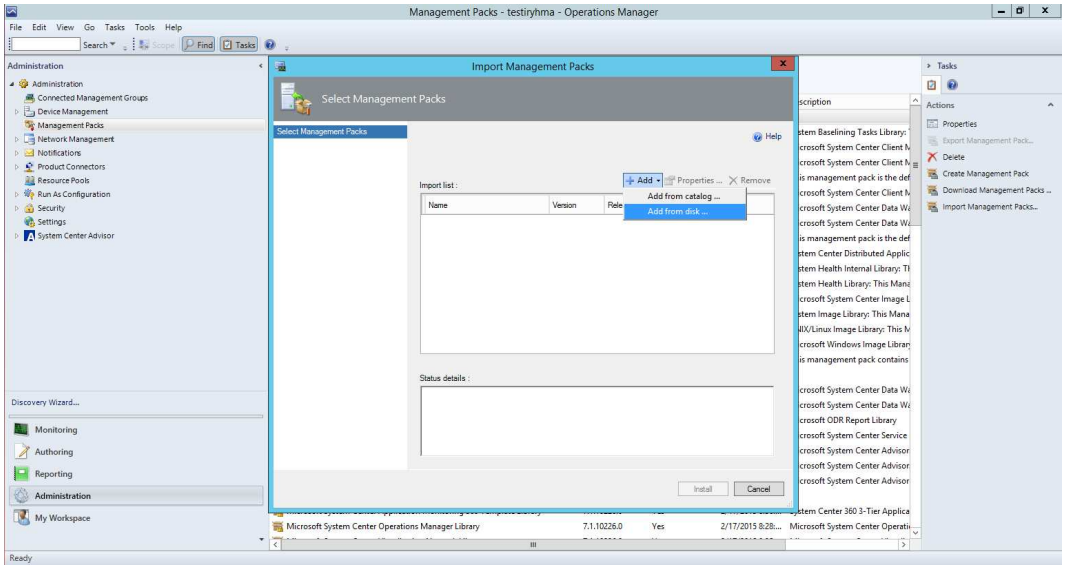
Hallintapakettien asennukseen ja niiden tuottamien hälytyksien, varoitusten ja virheiden analysointiin kannattaa ehdottomasti varata aikaa ja tehdä kartoitus huolellisesti. Jos virheellisiä tai turhia hälytyksiä tulee jatkuvasti useammasta kohteesta, SCOM-hallintapaneelin hälytysruutu täyttyy äkkiä epäollennaisesta tiedosta. Ensimmäisinä hallintapaketteina asennetaan SQL server 2012, Windows Server 2012 R2 –käyttöjärjestelmän, Active Directory ja Windows Server DNS hallintapaketit, jotta nähdään ettei omassa SCOM 2012 R2 -ympäristössä ole mitään vialla. Seuraavaksi asennetaan muut tarvittavat hallintapaketit esimerkiksi Citrix Edgesight, Microsoft App-V, DHCP ja loput mitä halutaan valvoa. Itse luoduista hallintapaketeista tulisi ottaa varmuuskopioinnit (liite 16) säännöllisesti SCOM 2012 R2 -tietokantojen ohella (liite 16).

Valmiin hallintapaketin asennus aloitetaan lataamalla asennuspaketti etukäteen esimerkiksi Windowsin omasta palvelusta ja otetaan se käyttöön SCOM 2012 R2 -järjestelmässä (KUVIO 29). Vaihtoehtoisesti hallintapaketti voidaan valita suoraan katalogista. Mukautettuja hallintapaketteja on syytä varoa ja suhtautua erittäin kriittisesti, koska niihin voidaan helposti mukauttaa erilaisia haitallisia komentosarjoja.



KUVIO 29. SCOM 2012 R2:n hallintapaketin asennus

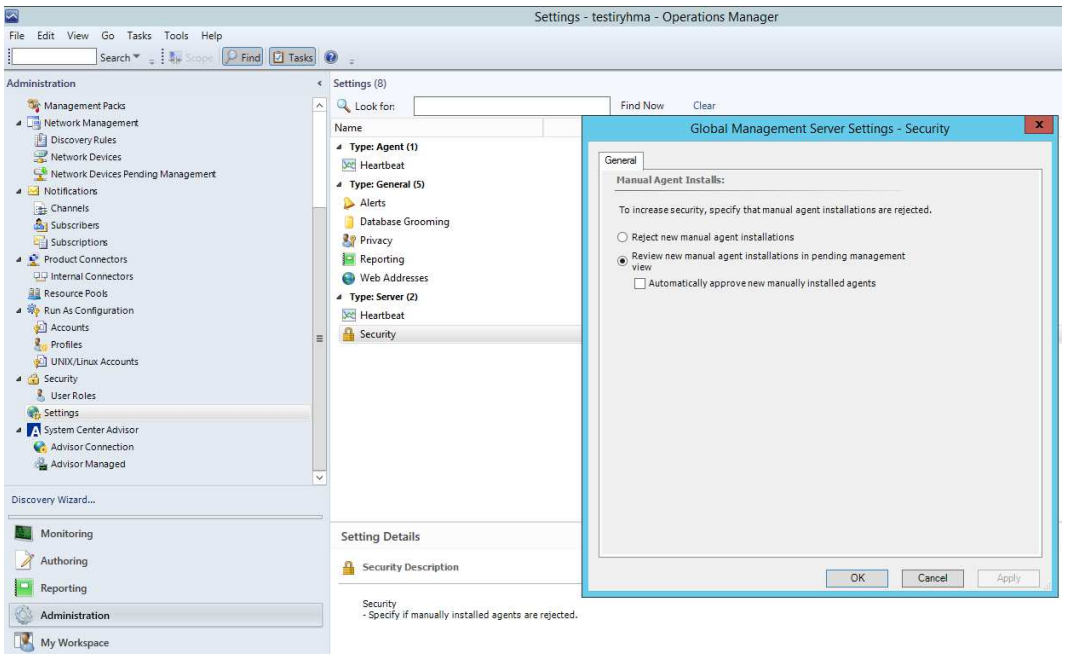
Seuraavaksi valitaan haluttu hallintapaketti, joka asennetaan. Valitaan Windows-palvelusta valmiiksi ladattu hallintapaketti paikalliselta kovalevyltä (KUVIO 30). Hallintapaketeilla saattaa olla riippuvaisuuksia myös toisiin hallintapaketteihin, jolloin helpointa on käyttää katalogia.



KUVIO 30. SCOM 2012 R2:n hallintapaketin valinta

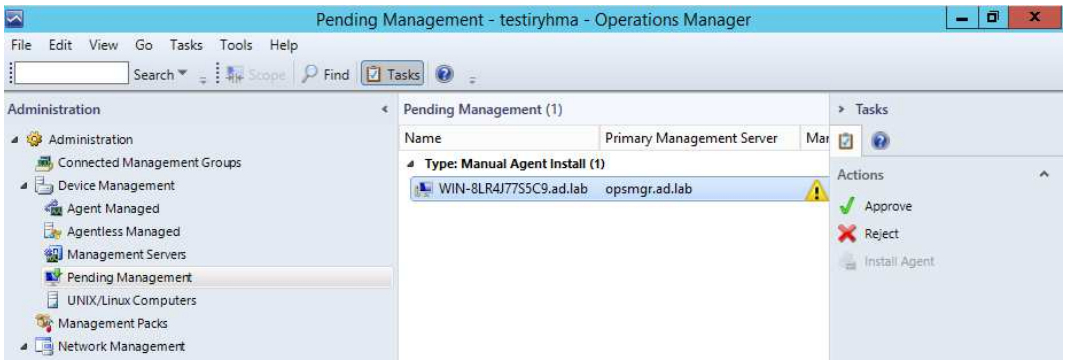
Kun valitut hallintapaketit ovat asennettuina, hallintapalvelin pystyy havainnoimaan hallintapaketin sisältämien sääntöjen avulla valvottavat kohteet. Esimerkiksi Windows Server 2012 R2 -hallintapaketin avulla voidaan havainnoida kaikki kyseisellä käyttöjärjestelmällä toimivat kohteet

ja lukea niiden suorituskykytietoja ja tehdä raportteja. Seuraavaksi määritetään hallintapalvelimelta, kuinka valvottavat kohteet lisätään hallintapalvelimelle valvontaan. Valitaan navigaationappuloista administration ja navigaatioikkunasta settings. Tulosruudusta valitaan settings, josta voidaan asettaa, kuinka manuaalisesti asennettujen agenttien kohdalla toimitaan. Valitaan agentit hyväksyttyväksi manuaalisesti, jolloin saavutetaan lisää tietoturvaa (KUVIO 31).



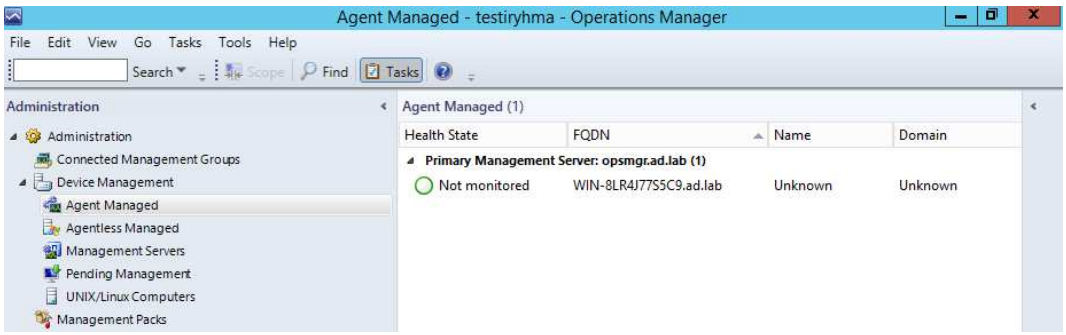
KUVIO 31. SCOM 2012 R2:n valvottavien kohteiden hyväksymistapa

Havaitut kohteet ovat käsittelyä vailla laitehallinnasa (device management). Havaittu kohde voidaan valita ja tarkastella sitä. Hyväksymällä kohde se lisätään valvontaan (KUVIO 32).



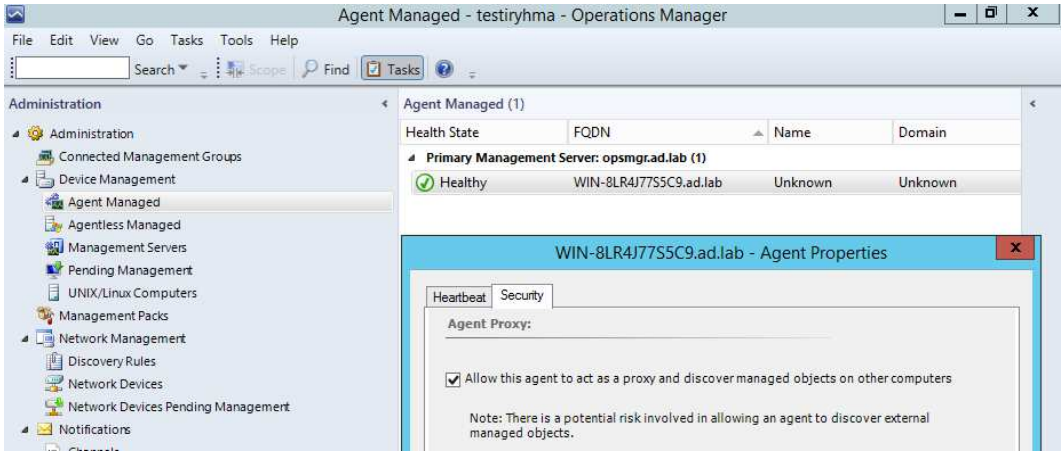
KUVIO 32. SCOM 2012 R2:n valvottavan kohteen hyväksyminen

Valvottavat kohde voidaan nyt havaita hallittavista kohteista (agent managed), tässä vaiheessa se ei ole vielä valvonnassa (KUVIO 33).



KUVIO 33. SCOM 2012 R2:n hallittavat kohteet

Valvottava kohde ja hallintapalvelin keskustelevat toistensa kanssa riippuen määritetystä heartbeat-välistä, joka on oletuksena 60 sekuntia. Kun rekisteröinti hallintapalvelimelle on tapahtunut ja kohde on täysin valvonnassa, kohteen tila (health status) muuttuu (KUVIO 34). Kyseessä olevan AD-palvelimen agentti asetetaan toimimaan välittäjänä. Tällöin agentti pystyy välittämään tietoa loogisista kokonaisuuksia, kuten klustereista.

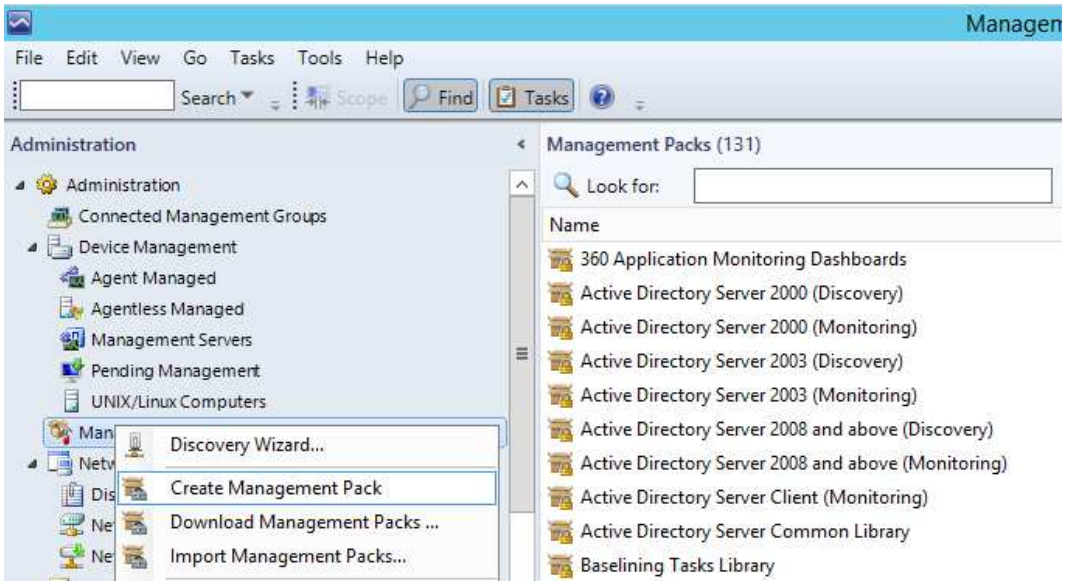


KUVIO 34. SCOM 2012 R2: agentti tiedon välittäjänä

7.4 SCOM 2012 R2: mukautetun ryhmän luominen

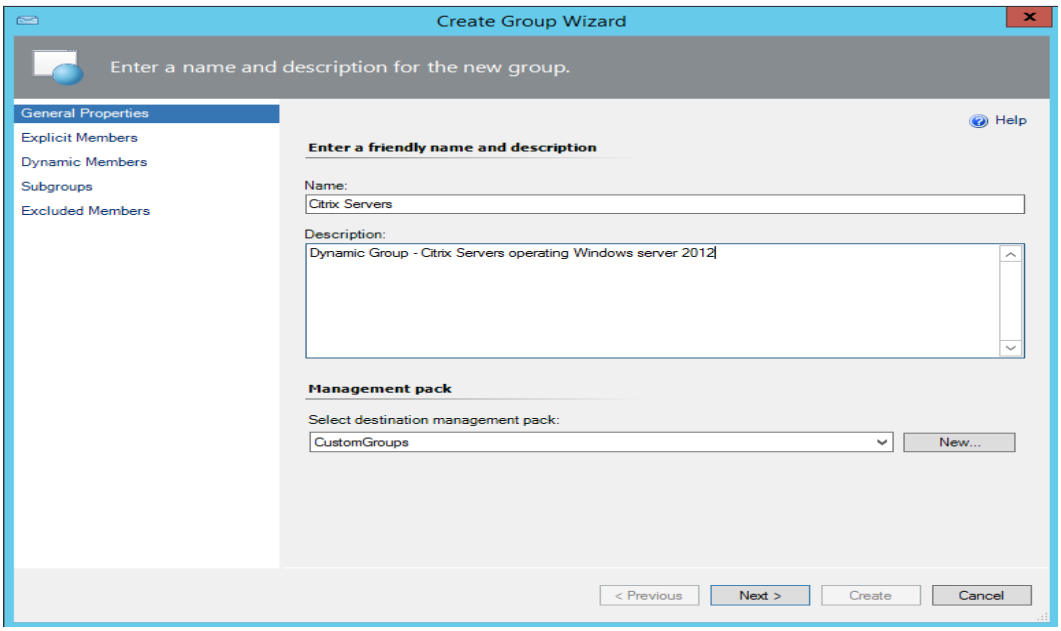
Kun hallintapaketteja asennetaan, valvotut kohteet lisätään vain hallintapaketissa ennaltamääritettyihin ryhmiin, jotka on määritelty

hallintapaketeissa erilaisin säännöin, kuten esimerkiksi kaikki Windows 2012 R2 -palvelimet. Mukautetulla ryhmällä voidaan luoda oma valvottava ryhmä kohteita esimerkiksi jostain suuremmasta kokonaisuudesta ja tarkastella jotain tiettyä suorituskykymittaria siitä ryhmästä. Aloitetaan luomalla oma hallintapaketti mukautetuille ryhmille (KUVIO 35).



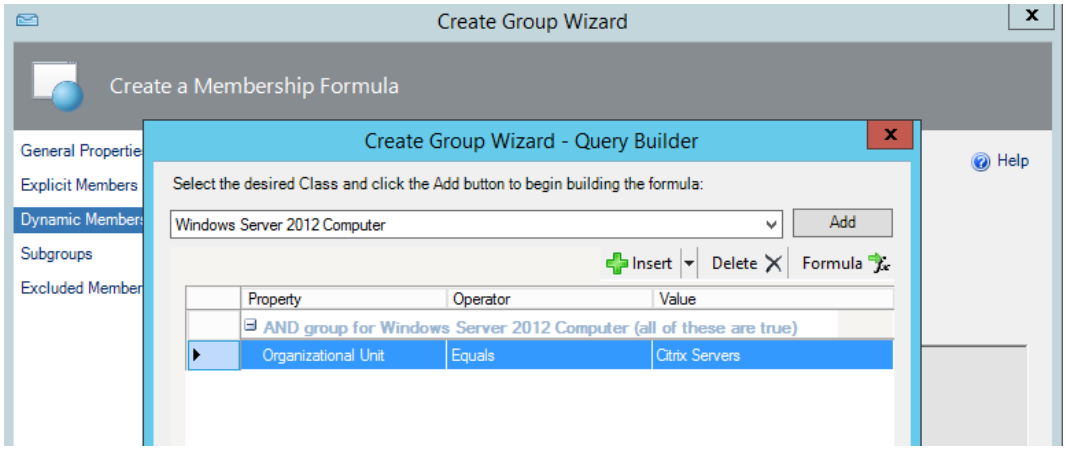
KUVIO 35. SCOM 2012 R2: hallintapaketin luonti

Valitaan mukautetuille ryhmille oma hallintapaketti, johon tallennetaan kaikki tehdyt muutokset koskien mukautettuja ryhmiä. Määritetään hallintapaketille oma nimi ”CustomGroups” ja määritetään uudelle ryhmälle nimi (KUVIO 36). Järjestelmään tehdyt uudet muutokset tulisi aina tallentaa erilliselle hallintapaketille ja välttää käyttämästä oletuksena olevia hallintapaketteja. Muutoksia on huomattavasti helpompi hallinnoida myöhemmin niitä vartavasten luotujen hallintapakettien avulla.



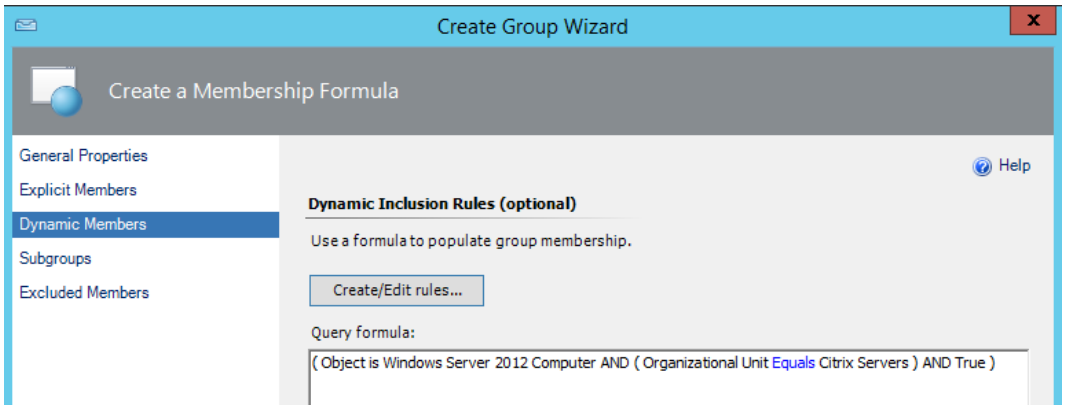
KUVIO 36. SCOM 2012 R2: mukautetun ryhmän nimeäminen

Luodaan esimerkkinä dynaaminen mukautettu ryhmä, jossa voidaan seurata kaikkia Citrix-palvelimia. Valitaan luokasta kaikki Windows 2012 -palvelinkoneet ja määritetään kaikki Active Directoryn Citrix Servers Organizational Unitiin kuuluvat tietokoneet kuulumaan ryhmään (KUVIO 37). Aina kun uusi Citrix-palvelin lisätään domainiin, Citrix Servers OU:hun, kuuluu se myös SCOM 2012 R2 Citrix Servers ryhmään. Vaihtoehtoisesti voitaisiin lisätä ryhmään esimerkiksi palvelimen DNS-nimellä tai vaikkapa jollakin tietyllä palvelimen rekisterissä sijaitsevan arvon perusteella.



KUVIO 37. SCOM 2012 R2: dynaaminen mukautettu ryhmä

Seuraavaksi tarkastellaan luotua ehtoa, jolla kohteet lisätään Citrix Server -ryhmään (KUVIO 38) ja edetään ryhmän luonnissa eteenpäin, kunnes ryhmä on luotu.

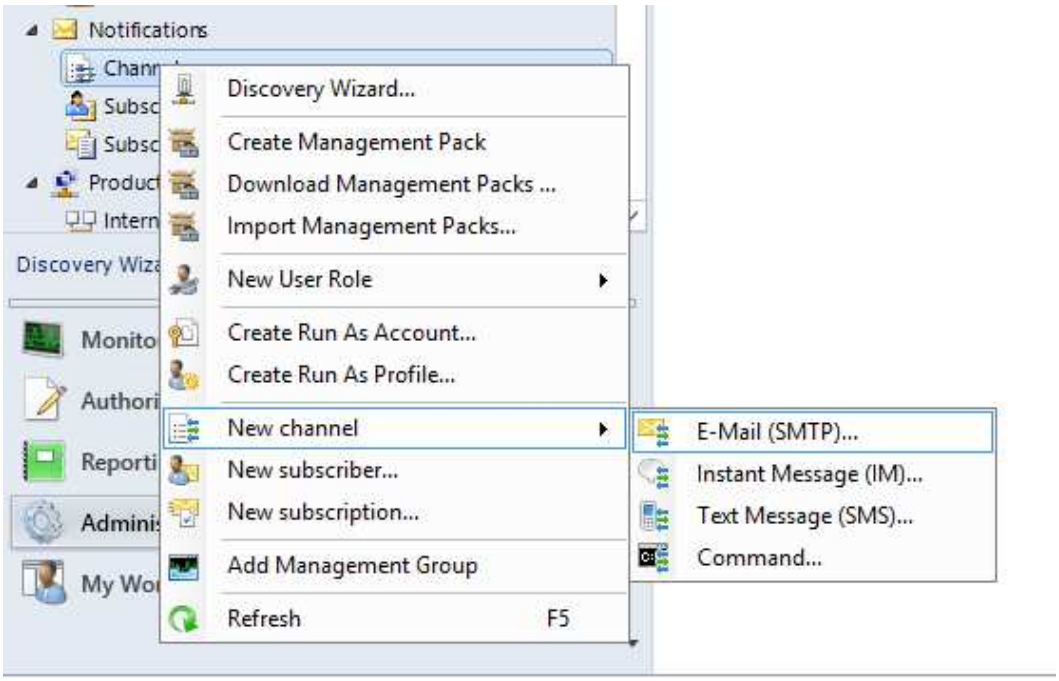


KUVIO 38. SCOM 2012 R2: mukautetun ryhmän kaava

Dynaaminen mukautettu ryhmä on nyt luotu ja se voidaan havaita julkaisun alta (authoring) kohdasta groups. Tarvittaessa sitä voidaan myöhemmin muokata.

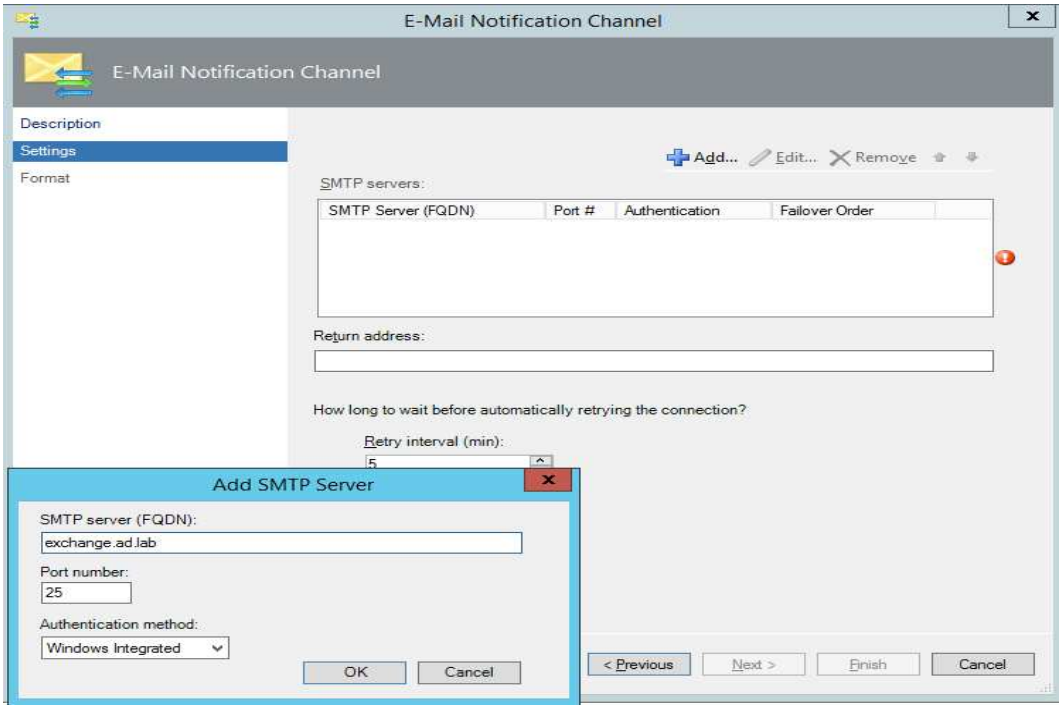
7.5 SCOM 2012 R2: hälytyksien ohjaus sähköpostiin

Ohjaamalla vakavat tuotantoa haittaavat ongelmat ja hälytykset sähköpostiin voidaan niihin reagoida huomattavasti nopeammin, kun ei mahdollisesti olla esimerkiksi työpisteellä ja tilanteesta voidaan saada nopeasti tarkempi käsitys. Aloitetaan luomalla sähköpostiviesteille oma kanava (KUVIO 39).



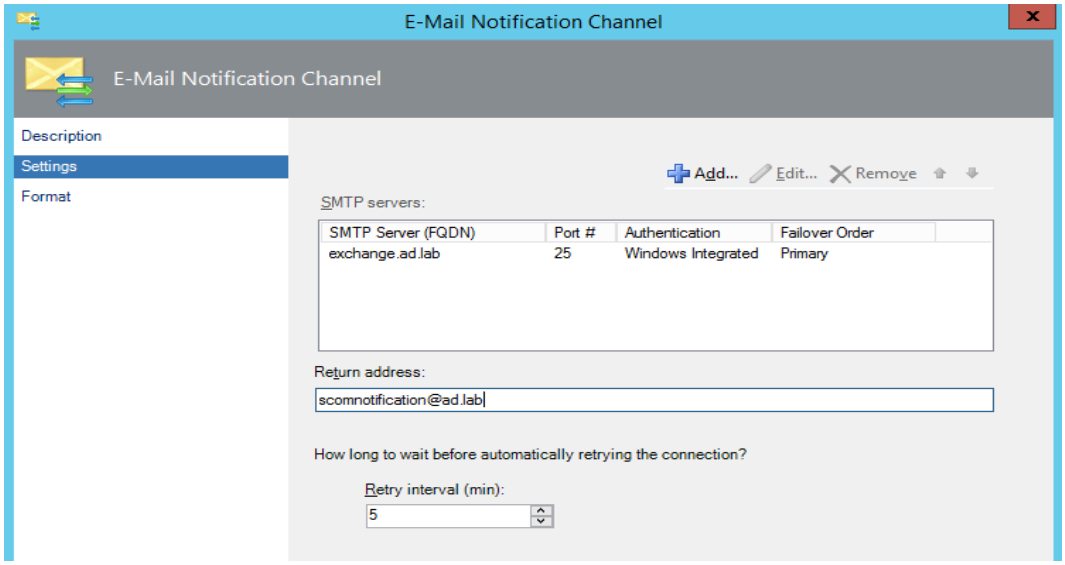
KUVIO 39. SCOM 2012 R2: sähköpostikanavan luonti

Nimetään seuraavaksi sähköpostille luotu kanava ja lisätään käytössä oleva sähköpostipalvelin käyttäen FQDN ja määritetään käytettävä portti. Valitaan tunnistautumisvaihtoehdoksi Windows tunnistautuminen anonyymin sijasta (KUVIO 40).



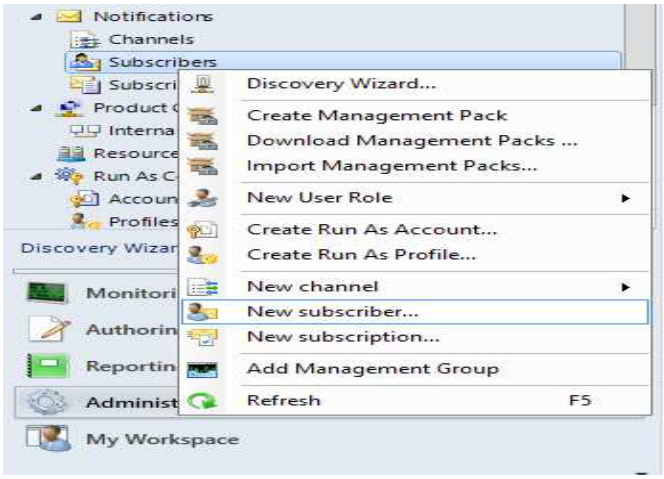
KUVIO 40. SCOM 2012 R2: sähköpostipalvelimen määritys

Sähköpostipalvelimen määrityksen jälkeen määritetään return address. Kyseisen osoiteen ei tarvitse olla oikea, mutta testiympäristössä luotiin sille oma tunnus. Tuotannollisessa ympäristössä tähän voitaisiin määrittää jakelulista (KUVIO 41).



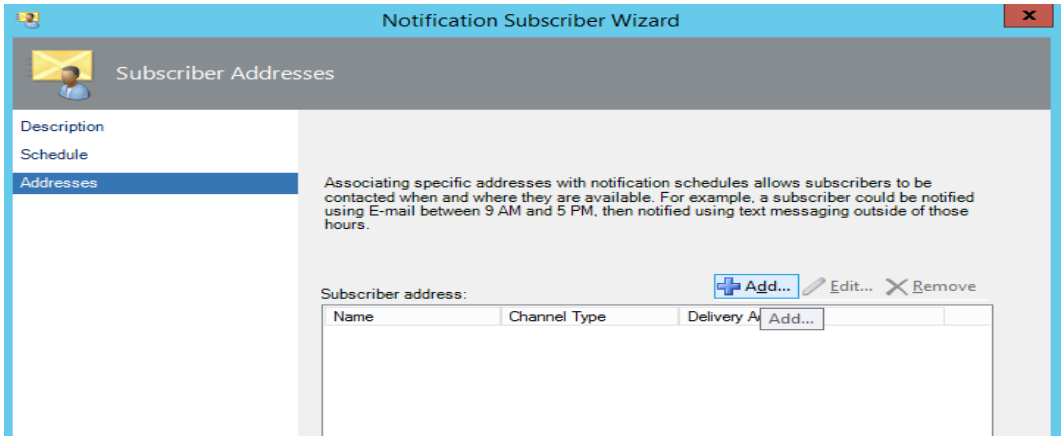
KUVIO 41. SCOM 2012 R2: sähköpostikanavan asetukset

Lopuksi tarkastellaan lähetetyn viestin muotoa. Viestien muotoa on mahdollista muokata halutessaan, mutta testiympäristössä käytetään vakioviestiä. Viestien tärkeyttä voidaan painottaa ja käytettävä viestin koodaus tyyppi voidaan myös tarvittaessa vaihtaa toiseksi. Kun kanava on luotu, SCOM tarvitsee osoitteen, jonne viestit lähetetään. Määritetään luodulle kanavalle tilaajat (subscribers) (KUVIO 42).



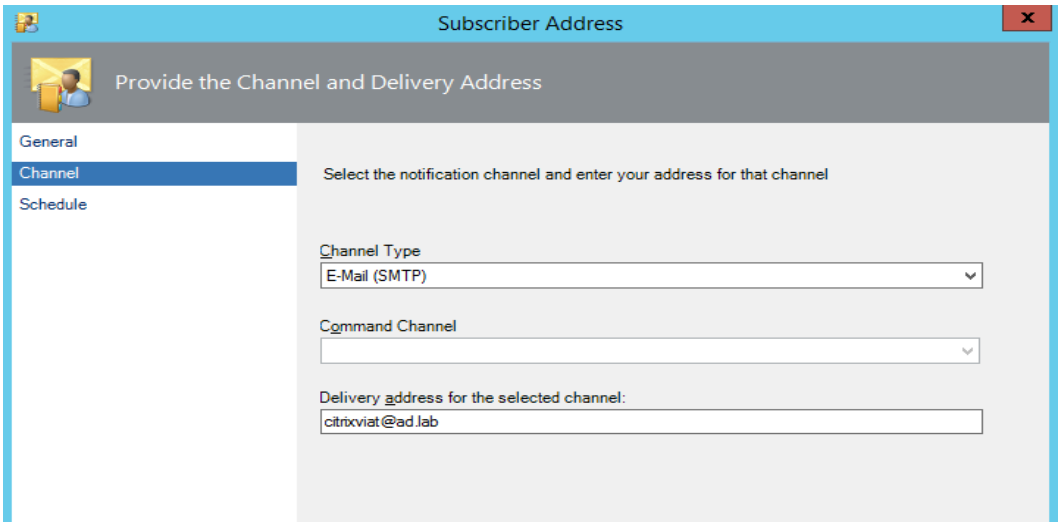
KUVIO 42. SCOM 2012 R2: uuden tilaajan luonti

Kuvion 43 mukaan määritetään ensin kohdasta Description tilaajan nimi ja kohdasta Schedule määritetään viestien lähettämisaikataulu niin, että viestit lähetetään aina kellonajasta riippumatta. Lisätään lopuksi halutut osoitteet Addresses-kohdan alta (KUVIO 43).



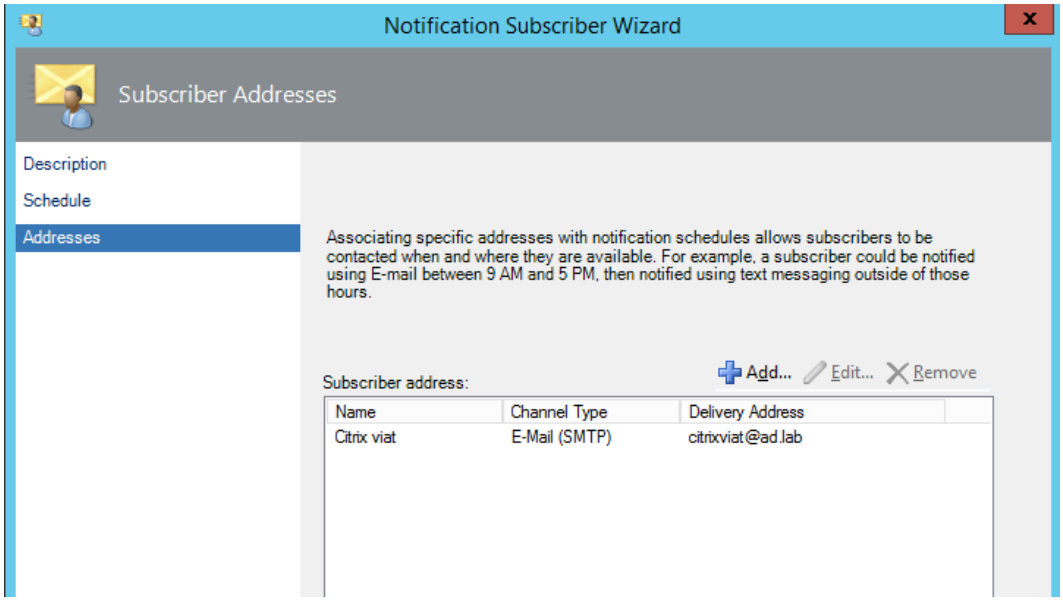
KUVIO 43. SCOM 2012 R2: tilaajan lisääminen

Seuraavaksi avautuu erillinen ikkuna, jossa määritetään tarkemmin tilaajan osoitteen nimi ja muut tiedot. Määritetään tilaajan osoitteen nimeksi ”Citrix viat”. Valitaan kanava, joka luotiin aiemmin, ja sidotaan se sähköpostiosoitteeseen. Sähköpostiksi voidaan esimerkiksi määrittää henkilökohtainen sähköposti tai tässä tapauksessa määritettiin yhteinen postilaatikko ”citrixviat@ad.lab”, johon useammalla käyttäjällä on oikeudet (KUVIO 44).



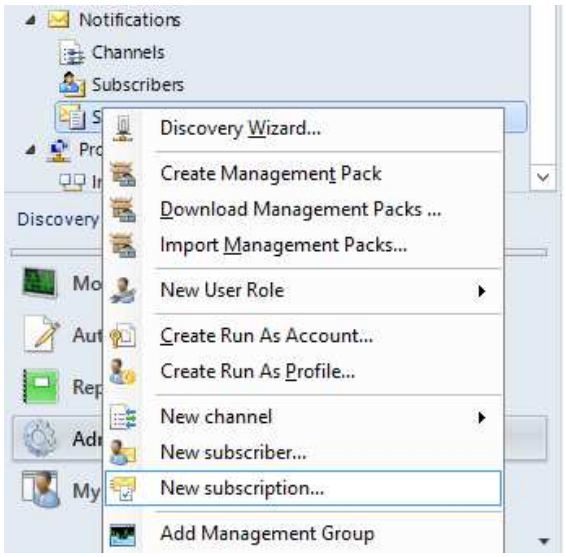
Kuvio 44. SCOM 2012 R2: tilaajan kanavan asetukset

Määritetään jälleen lähetysaikataulu viesteille kohdasta Schedule. Valitaan viestit lähetettäväksi aina. Kyseinen aikataulu on sähköpostikohtainen. Aiemmin luotu lähetysaikataulu koskee luotua tilaajaa. Lopuksi luodaan tilaaja ja tarkistetaan tehdyt määritykset (KUVIO 45). Tilaajia voidaan luoda enemmän ja sitoa tilaajat eri kanaviin ja eri eri lähetysaikatauluihin.



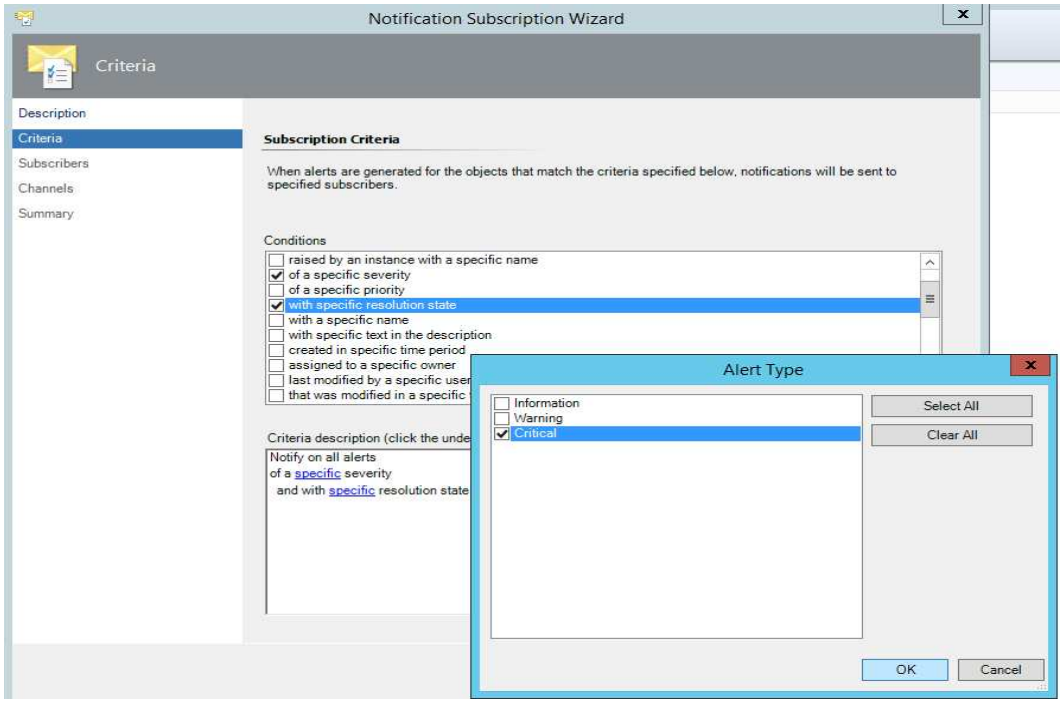
KUVIO 45. SCOM 2012 R2: luotu tilaaja

Kun kanava ja tilaaja ovat luotuna, niille pitää luoda ehdot, joiden täyttyessä viesti lähetetään tilaajalle (KUVIO 46).



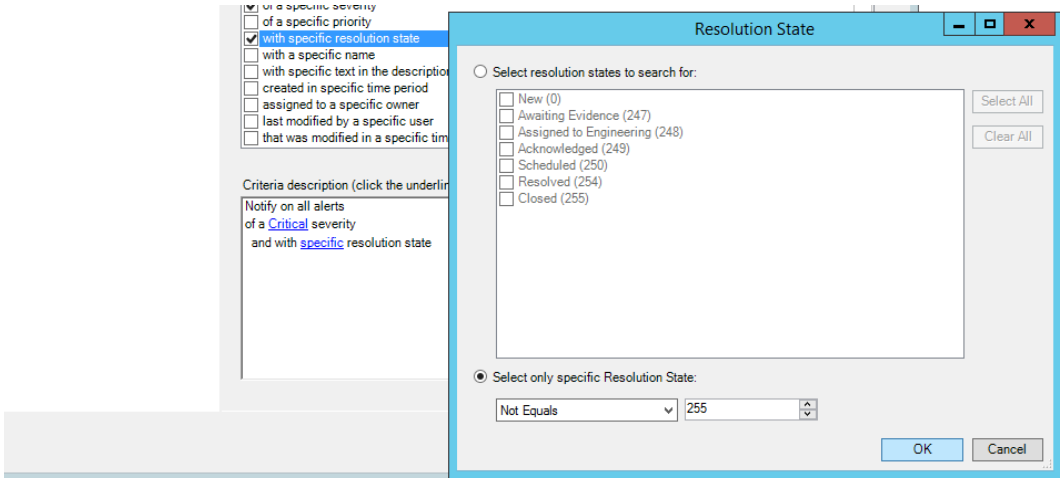
Kuvio 46. SCOM 2012 R2: uuden tilauksen luonti

Ensin määritetään kuvaava nimi kohdasta Description, jonka jälkeen määritetään määritetään ehdot, joiden toteutuessa viesti lähetään tilaajalle. Valitaan ehdoiksi hälytyksen vakavuus ja tila. Määritetään hälytyksen vakavuudeksi kriittinen (KUVIO 47).



KUVIO 47. SCOM 2012 R2: hälytyksen vakavuus

Määritetään vielä hälytyksen tila ja valitaan kaikki hälytykset, jotka eivät ole suljettuja eli niiden arvo on jokin muu kuin 255 (KUVIO 48).

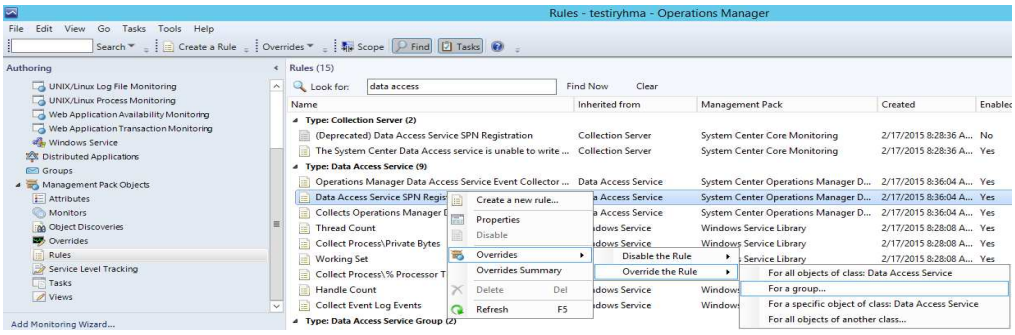


KUVIO 48. SCOM 2012 R2: hälytyksen tila

Varmistetaan vielä lopuksi määritetyt ehdot. Hälytyksistä, jotka ovat vakavuudeltaan kriittisiä ja eivät ole suljettuja, ilmoitetaan niistä tilaajalle. Ehtojen jälkeen lisätään vielä luotu tilaaja osaksi tilausta ja määritetään käytettäväksi luotu sähköpostikanava, jolla kyseisiä ehtoja käytetään. Kun kanava, tilaaja ja tilaus ovat luotuna onnistuneesti, hälytykset, jotka täyttävät luodut ehdot välitetään tilaajan sähköpostiin.

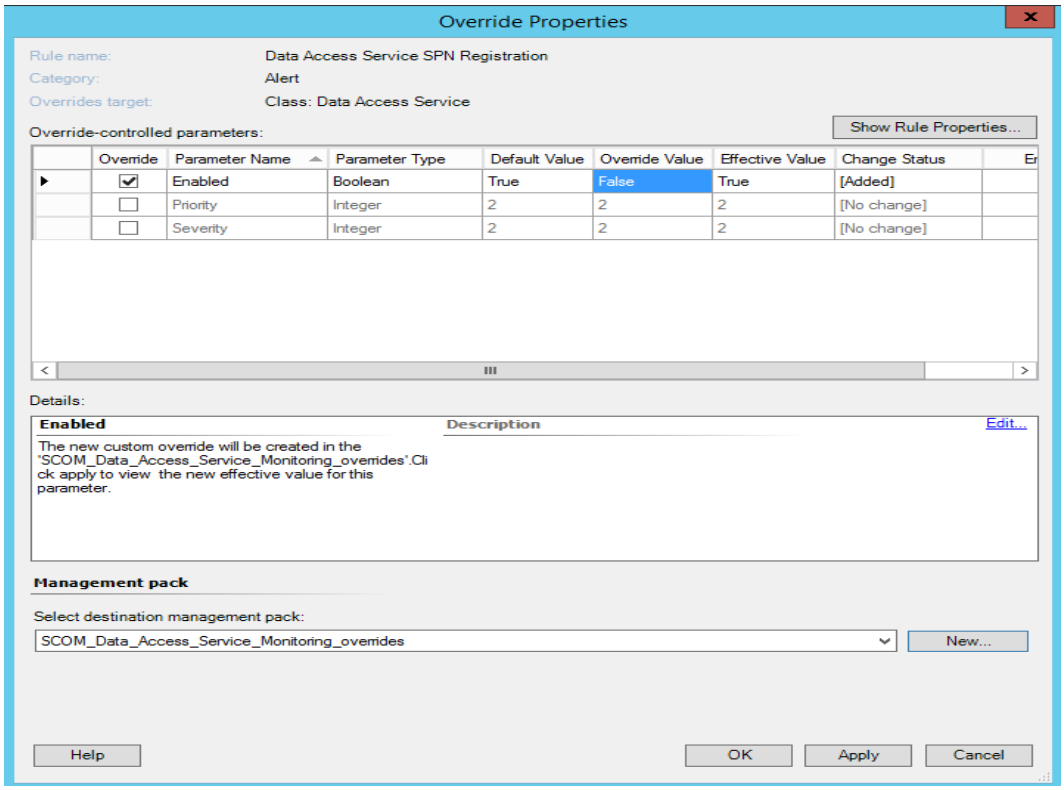
7.6 SCOM 2012 R2: Overrides

Overrides-ominaisuus on keskeisessä roolissa oman SCOM 2012 R2 -ympäristön muokkaamisessa. Hyödyntäen SCOM 2012 R2:n tarjoamaa override ominaisuutta, voidaan sillä rajata SCOM 2012 R2:n keräämää tiedon määrää ja rajata kerättyä tietoa. Kun hallintapaketteja asennetaan yksitellen, tulisi virheelliset ja tarpeettomat hälytykset seuloa läpi ja ohittaa ne käyttäen override-toimintoa. Override mahdollistaa säännön, monitorin, kohteiden etsinnän tai suorituskykylaskureiden attribuutin muokkaamisen. Kun kriittisiä hälytyksiä käydään läpi testiympäristössä, voidaan sieltä esimerkkinä seuloa väärä hälytys ”Data Access Service SPN Not Registered”. Kyseessä on testiympäristössä ilmestyvä bugi tai virheellinen hälytys. Kyseinen hälytys tarkistettiin aiheettomaksi testiympäristössä ja varmistettiin vielä toisesta lähteestä se virheelliseksi. Ennen kuin kriittisiä hälytyksiä sivuutetaan, on niistä oltava täysi varmuus ja mieluiten vahvistus myös muista lähteistä. Virheellinen hälytys, joka toistuu jatkuvasti, voidaan sivuuttaa menemällä kohtaan authoring ja valitsemalla rules. Etsitään kyseinen sääntö hakutoiminnolla ja sivuutetaan kyseinen sääntö koko ryhmältä (KUVIO 49).



KUVIO 49. SCOM 2012 R2: säännön sivuuttaminen

Valitaan override-kohta ylhäältä ja määritetään override-arvoksi false (KUVIO 50). Jos kyseessä olisi jokin attribuutti, sen arvoa voitaisiin halutessa muuttaa myös. Kun sääntöjä tai muita ominaisuuksia sivuutetaan, erillinen hallintapaketti tulisi aina luoda tai vaihtoehtoisesti tallentaa jo olemassaolevaan mukautettuun hallintapakettiin. Muutoksia ei pitäisi tehdä alkuperäiseen hallintapakettiin vaan luodaan alkuperäisen hallintapaketin rinnalle oma valitsemalla management pack kohdasta new (KUVIO 50). Tällä tavalla voidaan muutoksia paremmin hallinnoida tarvittaessa. Luodaan oma hallintapaketti muutoksille, jotka koskevat SCOM Data Access Service Monitoringia. Annetaan uudelle hallintapaketille myös alkuperäistä hallintapakettia sivuuttaen kuvaava nimi. Määritetään myös luodulle hallintapaketille täsmentävä kuvaus.



KUVIO 50. SCOM 2012 R2: säännön sivuuttamisen määritykset

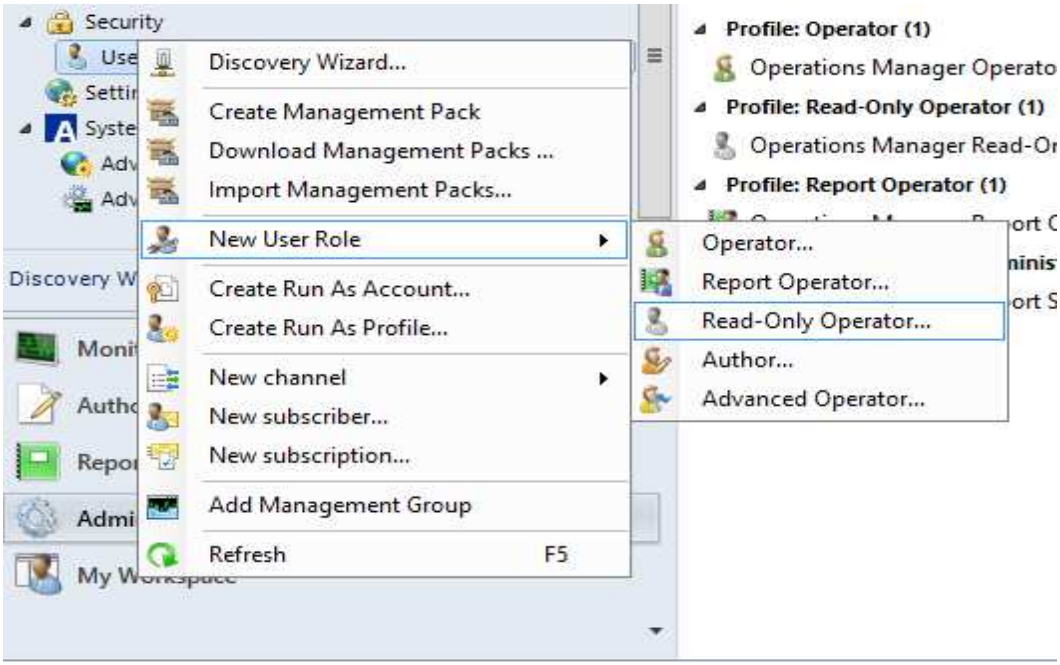
Nyt säännön sivuuttaminen voidaan ottaa käyttöön. Tehdyt määritykset tallentuvat luotuun hallintapakettiin. Kun olemassaoleva hälytys suljetaan, kyseistä sääntöä ei enää huomioida ja uutta hälytystä ei enää synny. Monitorien ja kohteiden arvoja voidaan tarvittaessa säätää. Kun

hallintapaketteja asennetaan, niiden mukana tulleet arvot eivät aina ole optimaalisia omaan ympäristöön, jolloin niitä voidaan muokata ja tallentaa erilliseen hallintapakettiin. Tämä onkin suotavaa oman ympäristön hallinnassa ja järjestelmän muokkaamisessa omaan ympäristöön sopivaksi.

7.7 SCOM 2012 R2: käyttäjien luonti

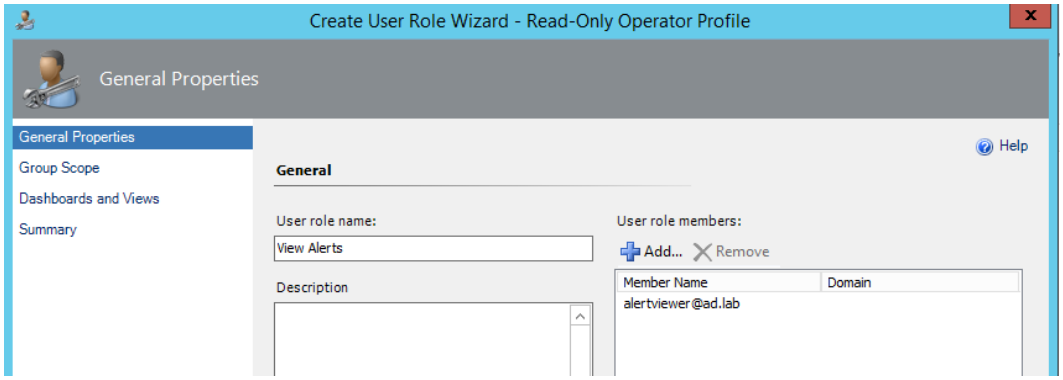
Tietoturvanäkökulmasta olisi jokaiselle käyttäjälle sidottava käyttöä vastaavat oikeudet. Esimerkiksi yrityksen toisen yksikön henkilö vaikka asiakasrajapinnasta voi tarvita oikeudet nähdä meneillään olevat hälytykset, jotta hän olisi perillä mahdollisista vikatilanteista. Toisenlaisena esimerkkinä esimies voi tarvita käyttäjätunnukset, jotta hän voisi koostaa raportteja tilastointia varten.

Luodaan käyttäjä, jolla on oikeudet seurata meneillään olevia hälytyksiä. Käyttäjän profiiliksi valittiin Read-Only Operator, koska kyseinen käyttäjä tarvitsee lukuoikeudet hälytyksiin ja näkymiin rajatuin oikeuksin (KUVIO 51).



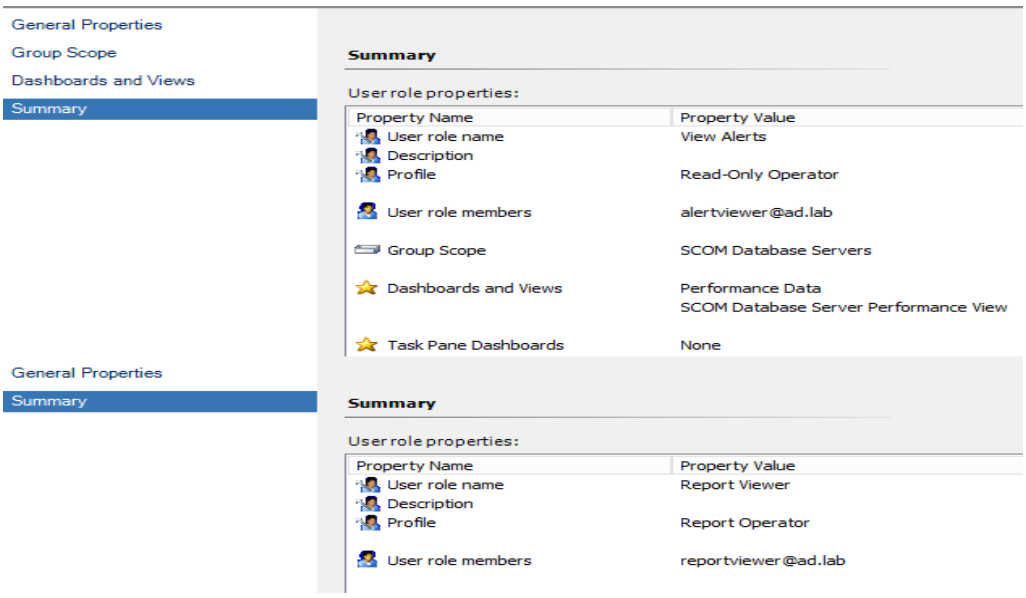
KUVIO 51. SCOM 2012 R2: käyttäjäroolin luominen

Määritetään seuraavaksi käyttäjäroolille nimi ja sidotaan käyttäjärooliin domain-tunnus (KUVIO 52)



KUVIO 52. SCOM 2012 R2: käyttäjäroolin määritykset

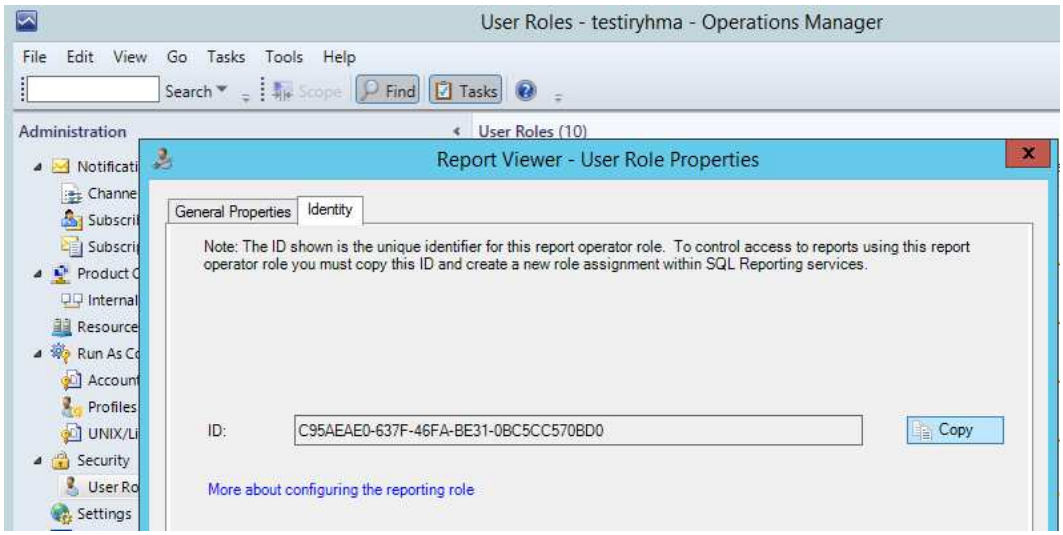
Seuraavaksi määritetään, mihin ryhmiin ja näkymiin käyttäjällä on oikeudet. Oikeudet voidaan rajata jo olemassaolevien ryhmien tai näkymien mukaan tai voidaan vaihtoehtoisesti luoda ryhmät tai näkymät käyttäjän mukaisesti. Valitaan käyttäjälle oikeudet SCOM-tietokantapalvelin-ryhmään sekä oikeudet näkymistä suorituskykytietoon ja SCOM-tietokantapalvelin näkymään. Lopuksi voidaan vielä tarkastella tehtyjä määrityksiä käyttäjän alertviewer osalta. Luodaan myös samalla raportointia varten oma käyttäjärooli ja sidotaan se käyttäjälle reportviewer (KUVIO 53).



KUVIO 53. SCOM 2012 R2: luodut käyttäjäroolit

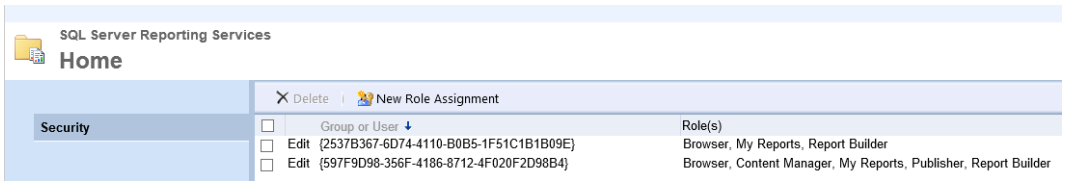
7.8 SCOM 2012 R2: raportointi

Raportteja voidaan lukea helposti selaimen avulla kirjautumalla raportointipalvelimelle. Sitä ennen joudutaan kuitenkin luomaan käyttäjälle reportviewer, oikeudet raportointipalvelimelle. Käyttäjän oikeudet voidaan lisätä kopioimalla käyttäjän reportviewer ID (KUVIO 54) ja lisäämällä uusi käyttäjä kyseisellä ID:llä raportointipalvelimelle.



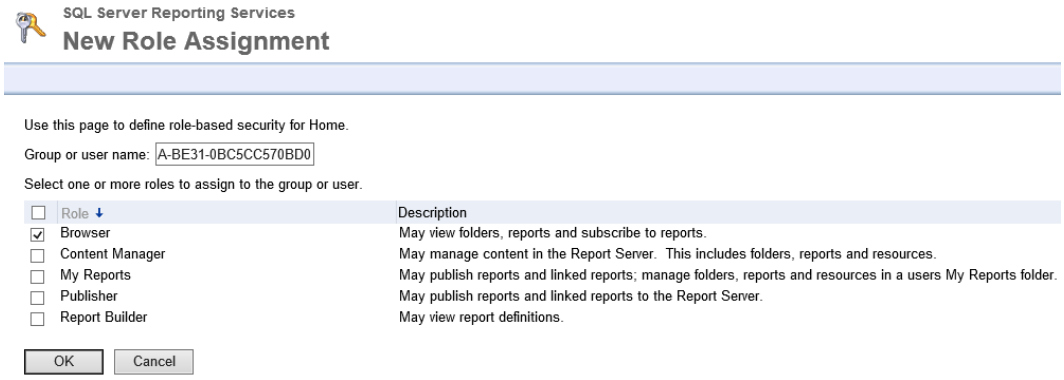
KUVIO 54. SCOM 2012 R2: käyttäjä ID

Seuraavaksi kirjaudutaan raportointipalvelimelle järjestelmäylläpitäjänä ja lisätään käyttäjä valitsemalla ensin hakemiston asetukset. Valitaan uusi käyttäjärooli palvelimelle ”New Role Assignment” (KUVIO 55).



KUVIO 55. SQL Server Reporting Services -uuden roolin lisäys

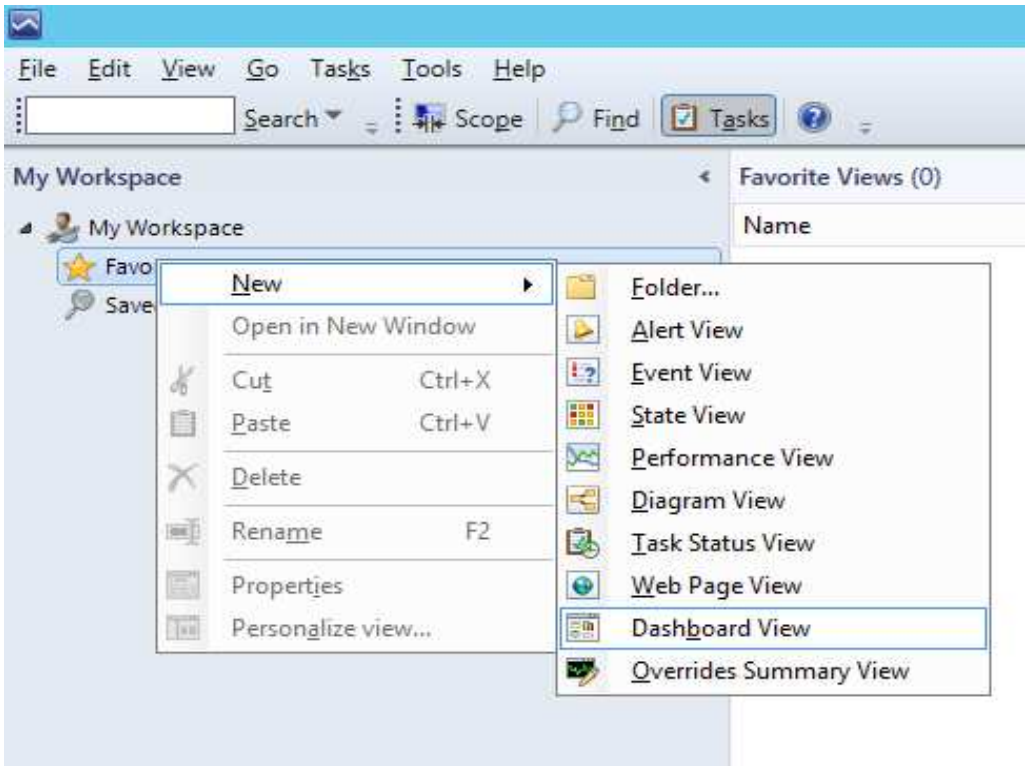
Liitetään seuraavaksi SCOM 2012 R2 reportviewer-käyttäjän ID, raportointipalvelimelle luodulle käyttäjäroolille. Määritetään roolin oikeudeksi selaaja (KUVIO 56). Reportviewer-käyttäjä pystyy nyt kirjautumaan raportointipalvelimelle ja selaamaan raportteja.



KUVIO 56. SQL Server Reporting Services: uuden roolin määrittäminen

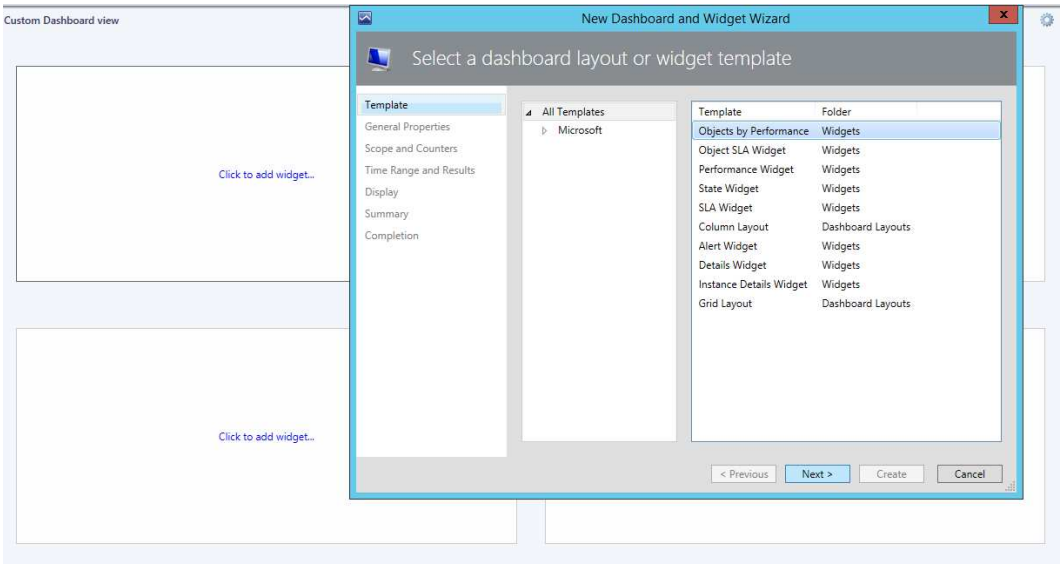
7.9 SCOM 2012 R2: oman näkymän luominen

Omien tai jaettujen näkymien luominen on ehdotonta, jotta voitaisiin toimia tehokkaasti omassa ympäristössä ja selvittää tärkeimmät ja olennaisimmat tiedot omasta valvotusta ympäristöstä. Informatiivisia mukautettuja näkymiä voidaan myös luoda tarvittaessa muille yrityksen eri yksiköille tehokkuuden lisäämiseksi. Luodaan seuraavaksi oma mukautettu näkymä (KUVIO 57).



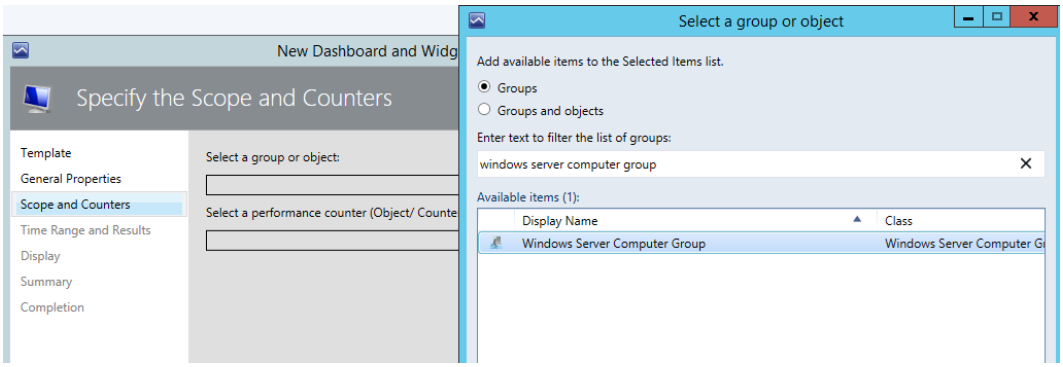
KUVIO 57. SCOM 2012 R2: dashboard-näkymän luonti

Valitaan kuvion 58 mukaisesti kohdasta template näkymäksi valmis taulukkomainen pohja (grid layout). Määritetään yleisistä asetuksista näkymälle kuvaava nimi ja tarkka kuvaus. Seuraavaksi valitaan omaan tarkoituksiin sopiva rakenne. Järkevintä olisi pyrkiä selkeyttämään näkymät niin, että ne olisivat mahdollisimman yksinkertaisia ja niistä näkyisi vain tarvittava tieto. Luodaan neljän solun taulukko, jonka jokaiseen soluun voidaan lisätä muokattuja pienoisnäkymiä (widget) (KUVIO 58). Valitaan yksi soluista ja lisätään pienoisnäkymä. Tarkoituksena on lisätä pienoisnäkymä, josta voi saada selville eniten muistia käyttävät Windows-palvelimet. Valitaan objects by performance.



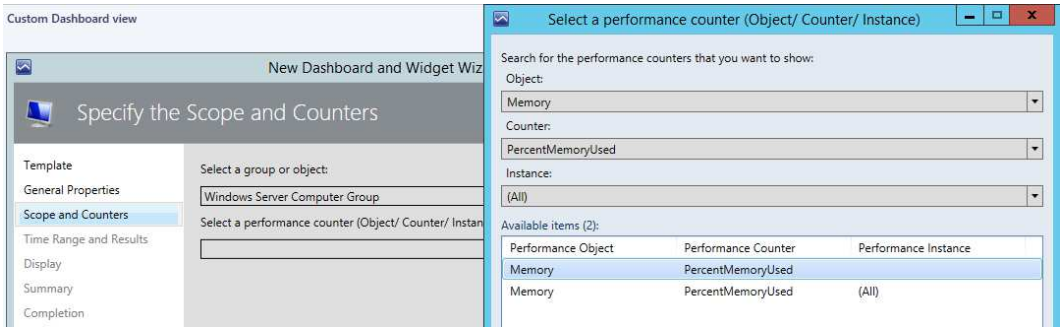
KUVIO 58. SCOM 2012 R2: oma pienoisnäkymä

Valitaan kuvaava nimi uudelle pienoisnäkymälle. Seuraavaksi valitaan ryhmät tai kohteet, joita halutaan valvoa. Valitaan kohteeksi Windows palvelinryhmä (KUVIO 59), joka kattaa yleisesti kaikki Windows Server -käyttöjärjestelmällä toimivat palvelimet. Vaihtoehtoisesti tähän voitaisiin laittaa esimerkiksi oma dynaaminen mukautettu ryhmä Citrix-palvelimia tai vaikkapa ryhmä tietokantapalvelimia.



KUVIO 59. SCOM 2012 R2: ryhmän valinta pienoisnäkymässä

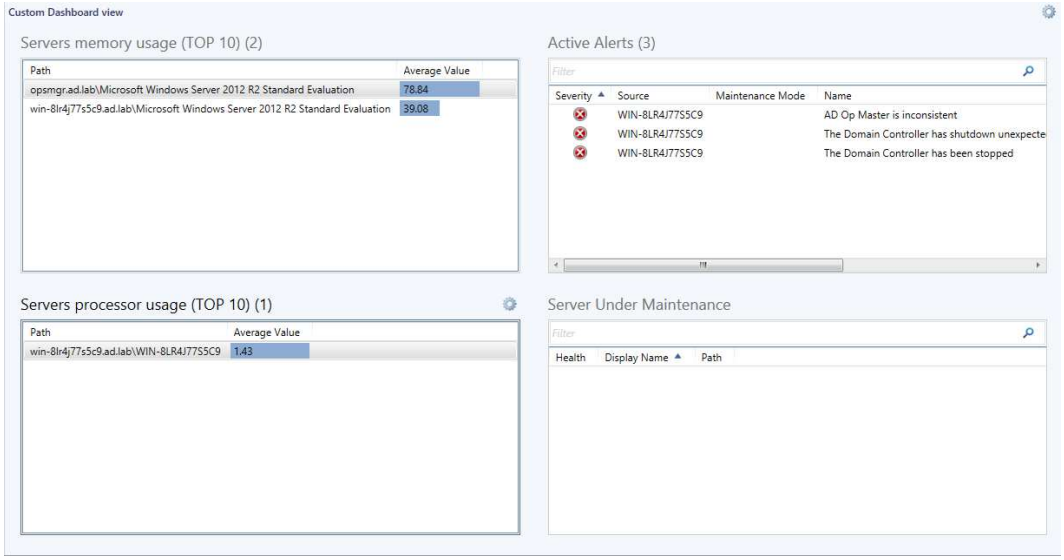
Kun ryhmä on valittu, valitaan kohde, jota mitataan kyseisestä ryhmästä. Valitaan kohteeksi muisti ja laskuriksi, se kuinka paljon muistia on käytettynä (KUVIO 60).



KUVIO 60. SCOM 2012 R2: pienoisnäkymän suorituskykylaskurit

Seuraavaksi määritetään, miltä ajanjaksolta tulokset näytetään. Valitaan suorituskykylaskureista näytettäväksi viimeisen viikon ajalta oleva palvelimien muistinkäyttö, jotta saataisiin kokonaisvaltaisempi kuva kuin vaikkapa yhden päivän ajalta. Määritetään myös näytettäväksi korkeimmat tulokset, koska halutaan seuloa suurimmat muistia käyttävät kohteet ja rajataan ne 10 kohteeseen. Lopuksi määritetään, mitä näytetään tulosten ohella pienoisnäkymän sisällä. Jätetään kohde (target) valitsematta, koska se veisi liikaa tilaa pienoisnäkymästä ja vaikeuttaa tarkastelua. Valitaan näytettäväksi polku ja keskimääräinen arvo. Annetaan mitta-asteikon säätyä automaattisesti.

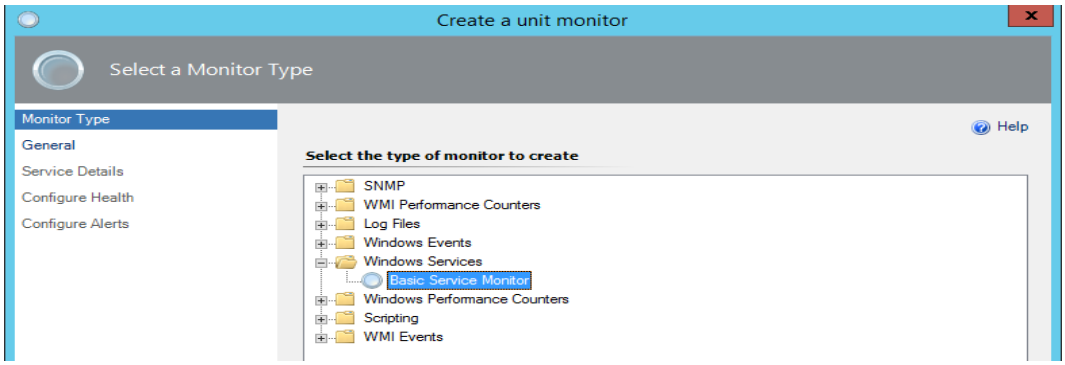
Lopuksi voidaan tarkastella luotua näkymää ja sen tuloksia. Samalla voidaan luoda muitakin pienoisnäkymiä kokonaiseen näkymään (KUVIO 61).



KUVIO 61. SCOM 2012 R2: neljän solun dashboard-näkymä

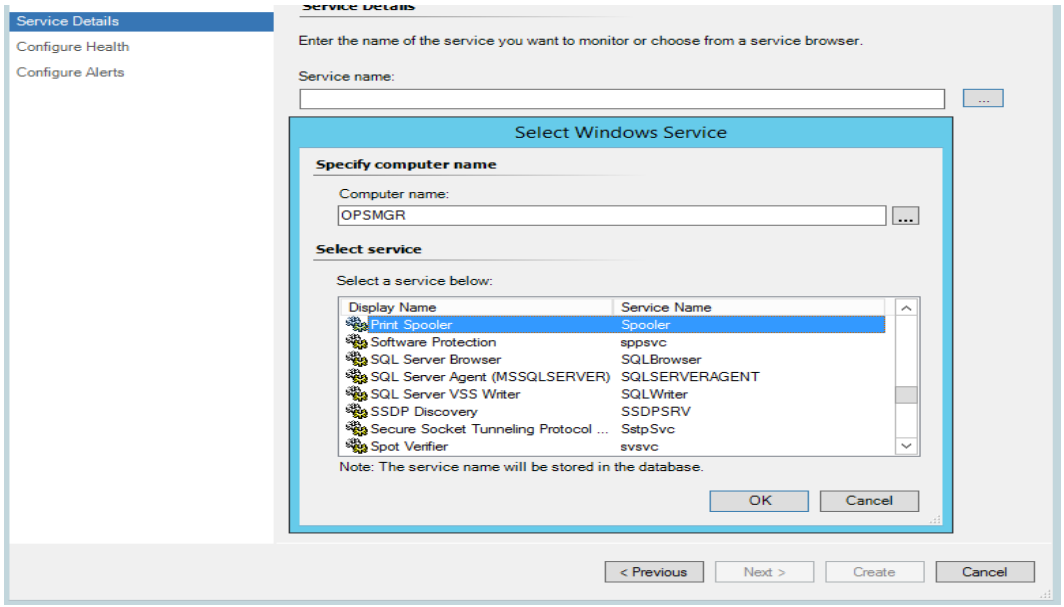
7.10 SCOM 2012 R2: palvelun automaattinen käynnistäminen

SCOM 2012 R2:n yhtenä suurena vahvuutena verrattuna esimerkiksi Citrixin EdgeSightiin on automatisointi. SCOM 2012 R2 mahdollistaa erilaisten käskyjen ja komentosarjojen ajamisen erilaisissa vika- tai diagnostiikkatilanteissa. Esimerkiksi Windowsin komentokehotteessa ajettavien käskyjen kautta voidaan käynnistää haluttuja palveluita uudelleen tai Microsoft Powershell -komentosarjoja hyödyntäen voidaan laittaa ryhmä tietokoneita huolto-tilaan. Jotta Windowsin palveluja voitaisiin käynnistää uudelleen, luodaan uusi Unit Monitor kohdasta Authoring ja Monitors – Create unit monitor. Automatisointia varten tulisi luoda oma erillinen hallintapaketti, esimerkissä käytetään ”Custom_Automation” hallintapakettia. Valitaan monitorin tyypiksi Windows Services alta Basic Service Monitor (KUVIO 62).



KUVIO 62. SCOM 2012 R2: valvojan tyypin valinta

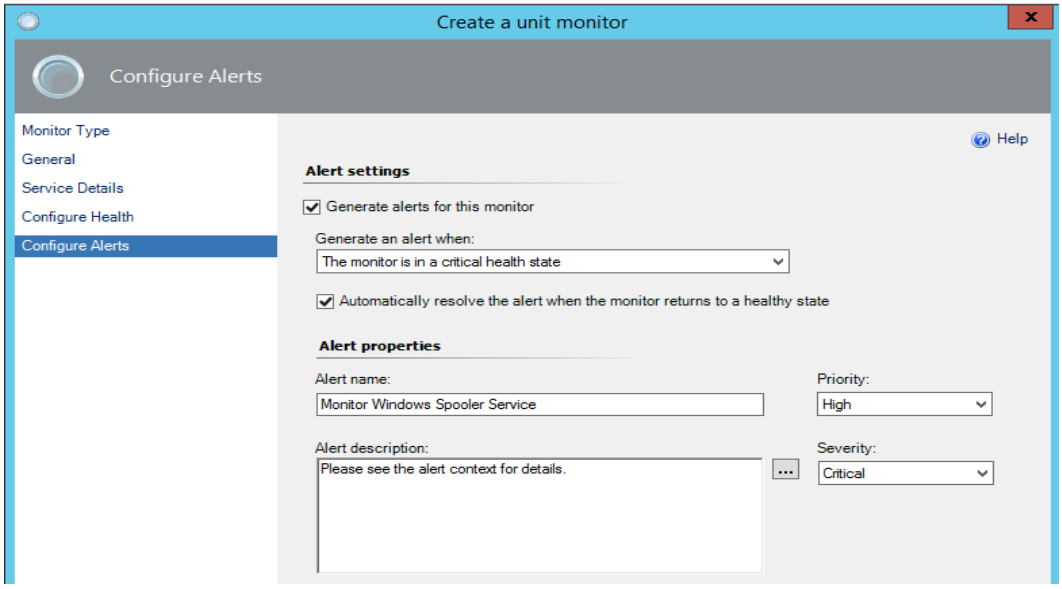
Seuraavaksi nimetään valvoja ja annetaan sille kuvaus. Käytetään jo luotua hallintapakettia ja valitaan monitorin kohteeksi kaikki Windows 2012 -palvelimet. Varmistetaan vielä, että monitor on käytössä. Jatketaan määrityksiä eteenpäin ja valitaan service-kohdasta jokin kohdetietokoneen palveluista. Esimerkissä käytetään harmitonta printer spooler -palvelua, joka otetaan valvonnan kohteeksi (KUVIO 63). Vaihtoehtoisesti voidaan valita haluttaessa jokin muu toimialueessa oleva kone ja sen palvelu, esimerkiksi jokin Citrix-palvelu (IMA Service), ja kohdistaa ryhmäksi kaikki Citrix-palvelimet, jotka ovat dynaamisessa ryhmässä osana.



KUVIO 63. SCOM 2012 R2: valvotun palvelun valinta

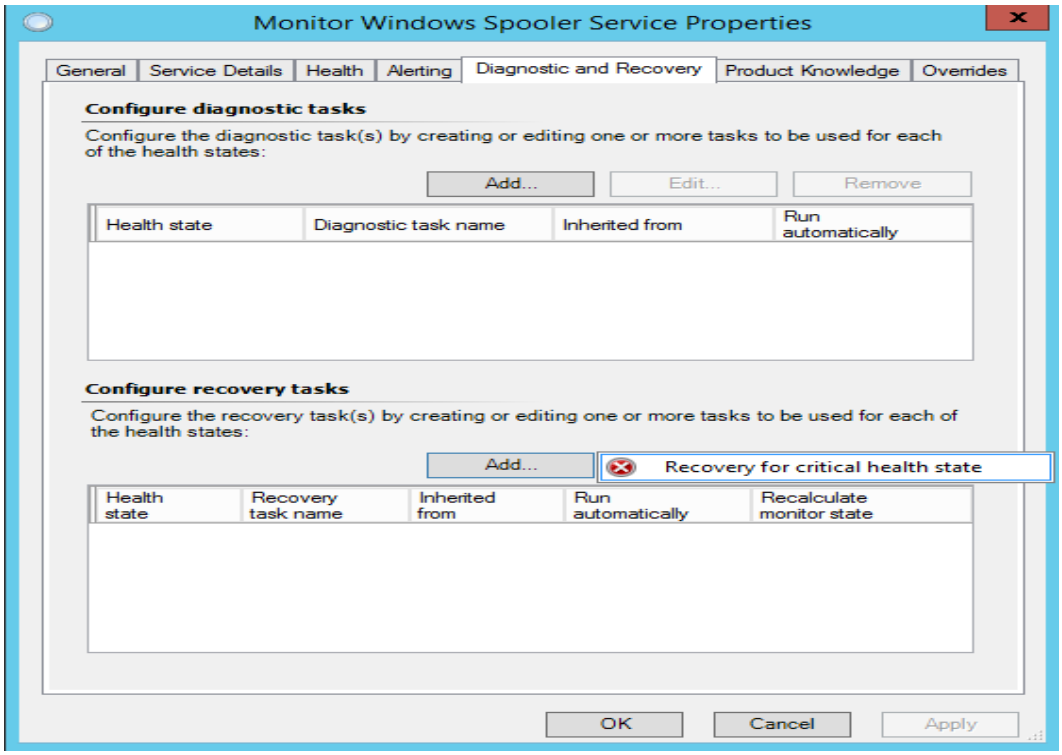
Määritetään vielä palvelun tilat oikein. Palvelun ollessa päällä sen tila on ”healthy” ja ”critical” palvelun ollessa pois päältä. Määritetään vielä lopuksi

hälytykseen liittyviä asetuksia. Hälytys luodaan, kun palvelu on mennyt pois päältä ja automaattisesti ratkaistaan tilanne hälytyksen ollessa taas päällä. Annetaan vielä hälytykselle kuvaava nimi ”Monitor Windows Spooler Service” ja laitetaan sille korkea prioriteetti ja hälytysasteeksi kriittinen (KUVIO 64).



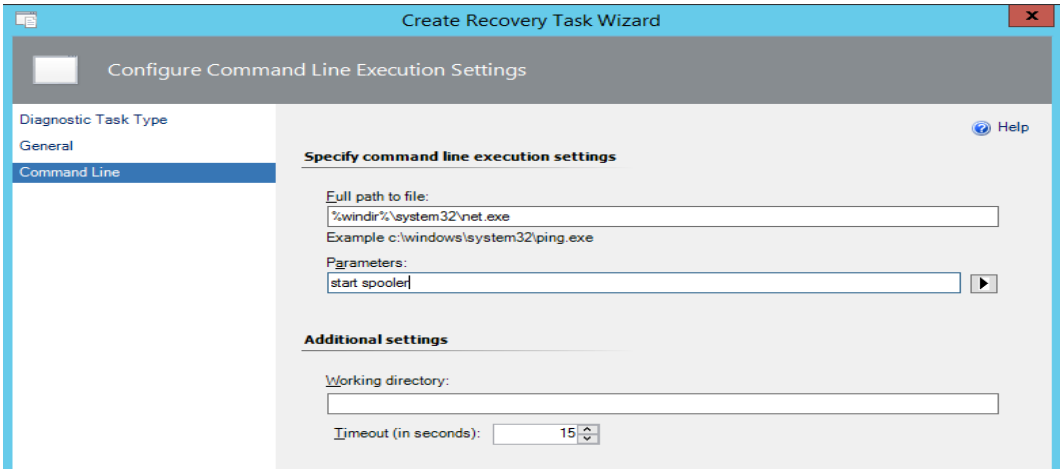
KUVIO 64. SCOM 2012 R2: valvojan hälytysasetukset

Seuraavaksi siirrytään tarkastelemaan luotua valvojaa kohdasta ”Authoring and monitors”. Valitaan luodusta valvojasta ”Diagnostics and Recovery” -välilehdeltä ”configure recovery tasks” (KUVIO 65) ja luodaan uusi tehtävä suoritettavaksi. Valitaan vikatilanteessa ajettavan tehtävän tyypiksi käsky ja määritellään muutokset tehtäväksi aiemmin luotuun hallintapakettiin.



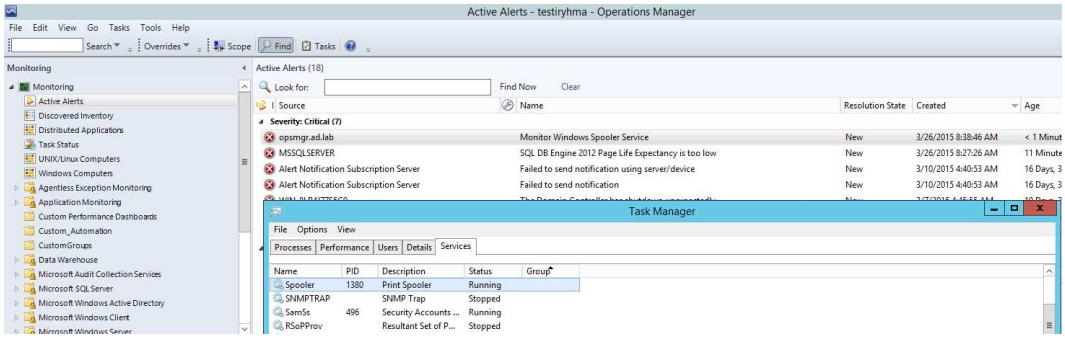
KUVIO 65. SCOM 2012 R2: tehtävän luonti vikatilanteelle

Nimetään luotava tehtävä ja määritetään se suoritettavaksi vikatilanteessa. Valitaan suoritettavan tehtävän kohteeksi Windows 2012 -palvelimet. Määritetään vielä tarvittava komento ja parametrit, joilla Windows Print Spooler -palvelu voidaan käynnistää. Määritetään poluksi Windows-asennushakemisto ja suoritettavaksi tiedostoksi ”net.exe” tiedosto ”start spooler”-parametrein (KUVIO 66). Kokonaisuudessaan käskyksi muodostuu siis ”net start spooler”.



KUVIO 66. SCOM 2012 R2: tehtävän komentosarja

Seuraavaksi voidaan testata kyseisen monitorin ja tehtävän toimintaa avaamalla Windowsin oma tehtävänhallinta ja pysäyttämällä Spooler -palvelu. Kun palvelu pysäytetään, SCOM 2012 antaa siitä hälytyksen ja suorittaa määritetyn komentorivin palvelun käynnistämiseksi uudelleen (KUVIO 67.).



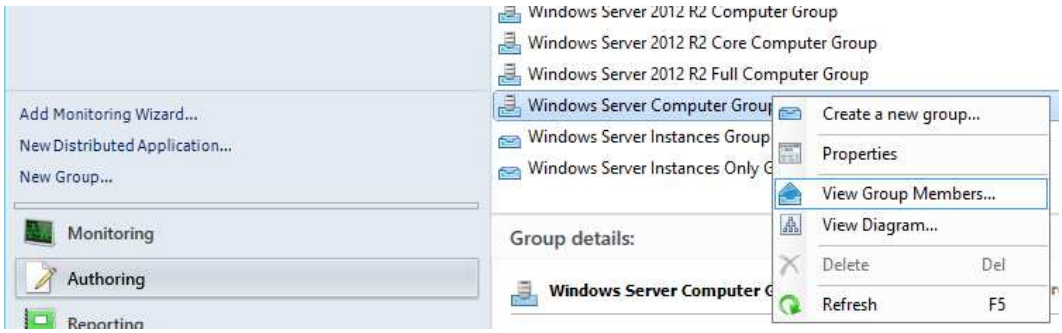
KUVIO 67. SCOM 2012 R2: palvelun uudelleenkäynnistys vikatilanteessa

7.11 SCOM 2012 R2: palvelimen huoltotilan automatisointi

Usein yrityksissä tehdään päivityksiä ja huoltokatkoja palvelimiin säännöllisin väliajoin tai jotkin palvelimet toimivat huomattavasti paremmin, kun ne käynnistetään uudelleen. Citrixin provisioidut palvelimet ovat yksi esimerkki palvelimista, joita täytyy tai suositellaan käynnistettäväksi usein ja säännöllisin väliajoin. Kun palvelimet käynnistetään uudelleen, hallintapalvelin havaitsee ettei agentti lähetä enää tietoa ja se luulee palvelimien olevan alhaalla. Tilanteesta aiheutuu suuri määrä turhia hälytyksiä. Kun tiedetään ajankohdat, jolloin palvelimien alasajoja tehdään, voidaan kyseiset palvelimet laittaa huoltotilaan automaattisesti kyseisinä ajankohtina.

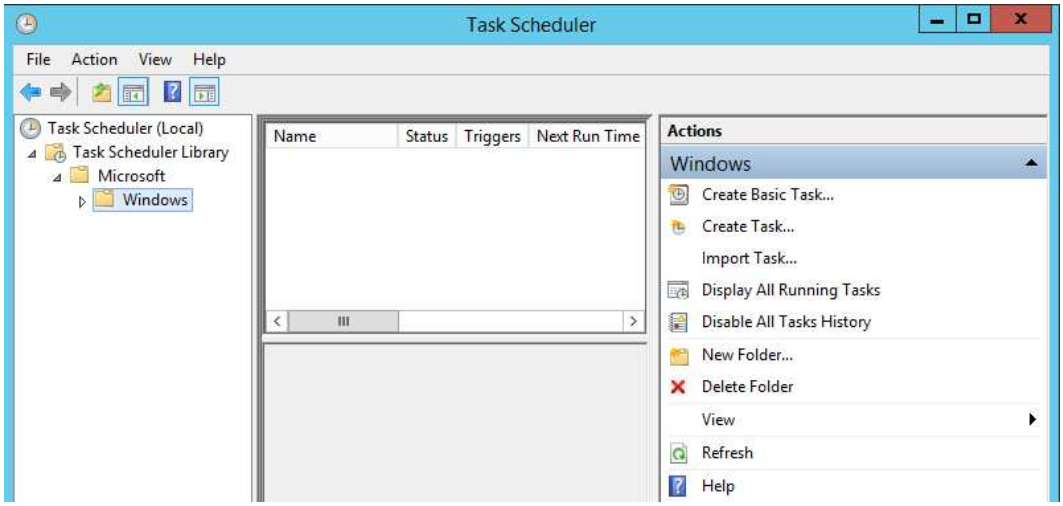
Seuraavaksi automatisoidaan tiettyyn ryhmään kuuluvat palvelimet menemään huoltotilaan, kun ne uudelleenkäynnistetään. Koska testiympäristössä ei ole suurta määrää palvelimia, käytetään kohderyhmänä kaikkia Windows palvelimia. Tarvittaessa kohteena voitaisiin myös käyttää dynaamista tai staattista ryhmää sisältäen provisioituja Citrix-palvelimia. Siirrytään SCOM 2012 R2:n konsolissa authoring-tilaan ja groups, josta voidaan katsoa ryhmän tarkka nimi

(KUVIO 68) ja siihen kuuluvat kohteet, joita huoltotila koskee. Automatisoinnissa käytetään hyväksi Microsoft Powershell -komentotulkkia, powershell-komentosarjaa ja batch-tiedostoa käskyttämään hallintapalvelinta.



KUVIO 68. SCOM 2012 R2: ryhmät

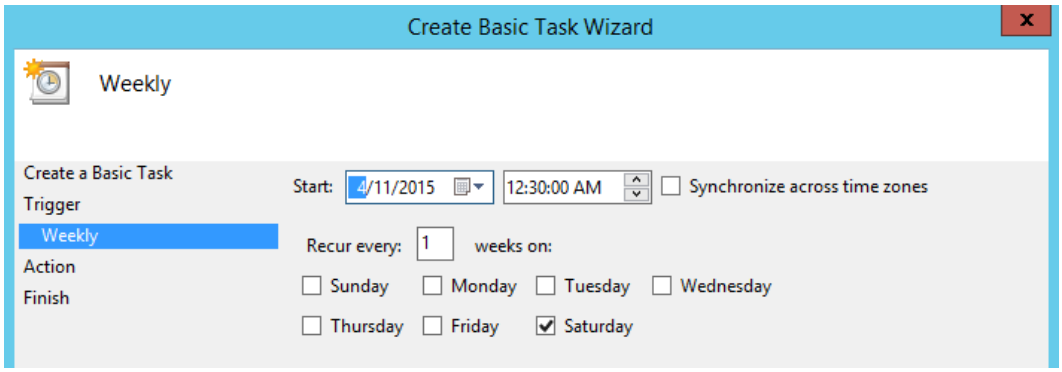
Seuraavaksi avataan Windows-käyttöjärjestelmän oma Task Scheduler, jolla voidaan ajastaa Windows suorittamaan erilaisia tehtäviä ajastetusti. Luodaan Task Schedulerissa tavallinen tehtävä (KUVIO 69).



KUVIO 69. Windows Server 2012 R2: ajastetun tehtävän luonti

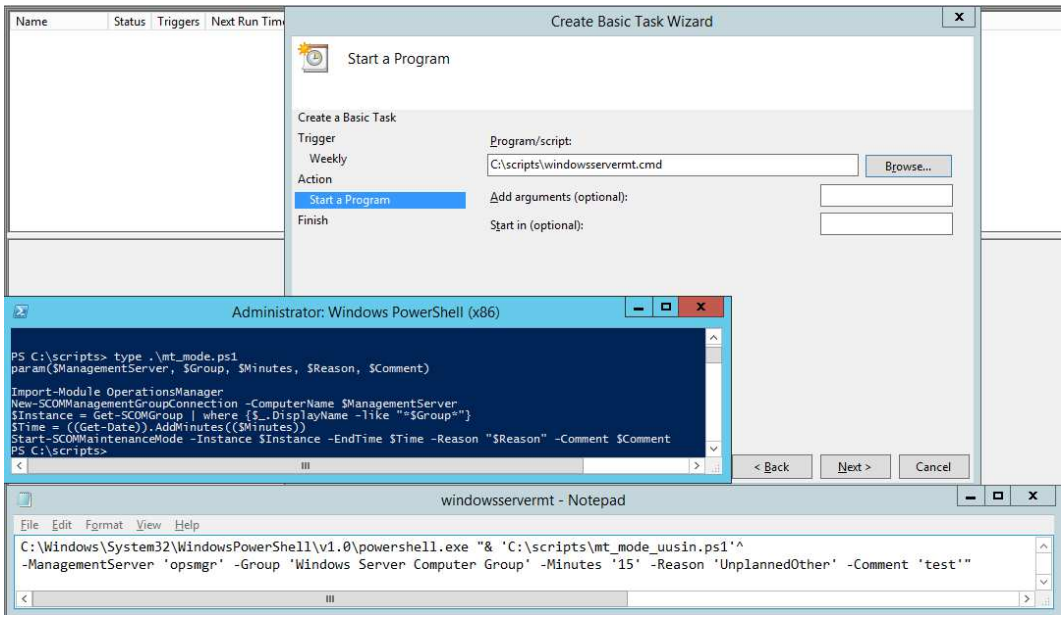
Annetaan tehtävälle mahdollisimman kuvaava nimi ja kuvaus, jotta jälkeenpäin voitaisiin helposti seuloa oikeat automatisoinnit. Jatketaan eteenpäin ja määritellään, kuinka usein mahdollinen palvelinten alasajo tai päivitys tapahtuu. Valitaan tehtävä suoritettavaksi viikottain tapahtuvaksi osana sovittua huoltokatkoa. Määritellään tarkempi aika ja päivä, jolloin tehtävä suoritetaan. Palvelinten uudelleenkäynnistys tapahtuu

testiympäristössä aina sunnuntaisin, yöllä kello 0.32. Palvelinten ajo huoltotilaan tapahtuu kello 0.30 (KUVIO 70), joten kohteille jää pari minuuttia aikaa muuttaa tilansa valvottavasta huoltotilaan.



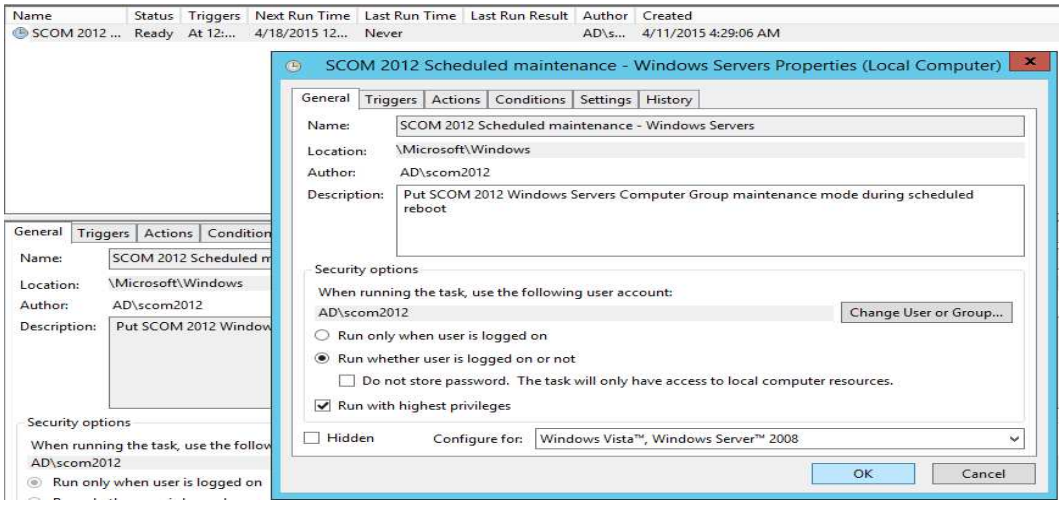
KUVIO 70. Windows Server 2012 R2: tehtävän suoritusajankohta

Määritetään seuraavaksi, millainen tehtävä suoritetaan. Koska kyseessä on komentosarja, valitaan suoritettavaksi ohjelma (program). Valitaan ohjelma, joka halutaan suorittaa. Automatisointia varten käytetään luotua powershell-komentosarjaa (liite 18), joka käynnistetään batch-tiedoston windowsservermt.cmd:n (liite 18) avulla. Valitaan suoritettavaksi ohjelmaksi windowsservermt.cmd-tiedosto. Batch-tiedostoon on määritelty muuttujat, jotka syötetään powershell-komentosarjalle. Powershell-komentosarjalle kerrotaan hallintapalvelimen nimi (opsmgr), huoltotilaan laitettavan tarkka ryhmän nimi (Windows Server Computer Group), huoltotilan kesto (15 minuuttia), syynä käytetään Windows Shutdown koodeja (UnplannedOther) ja kommentiksi jotain informatiivista (KUVIO 71).



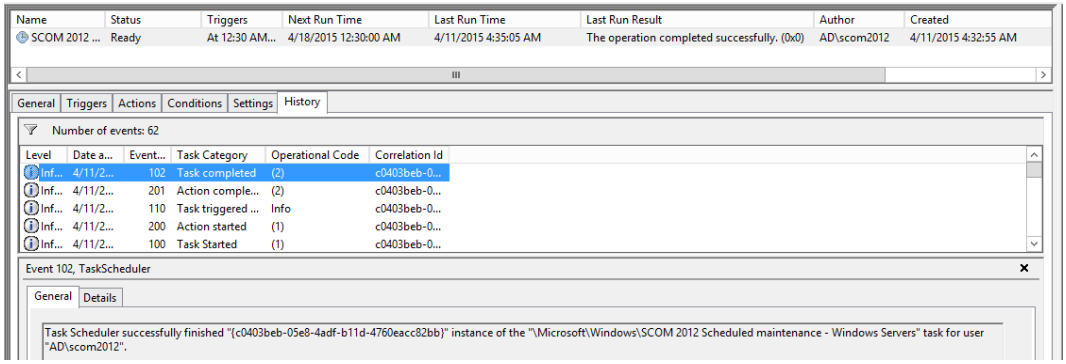
KUVIO 71. SCOM 2012 R2: ryhmän huoltotila ja komentosarjat

Tehdään vielä lopulliset määritykset luotua tehtävää varten. Valitaan tehtävästä asetukset (properties) ja määritellään general-välilehdeltä tehtävä käynnistettäväksi siitä huolimatta, onko käyttäjä kirjautunut palvelimelle vai ei. Määritetään myös tehtävä suoritettavaksi mahdollisimman korkeilla oikeuksilla ja hyväksytään muutokset (KUVIO 72).



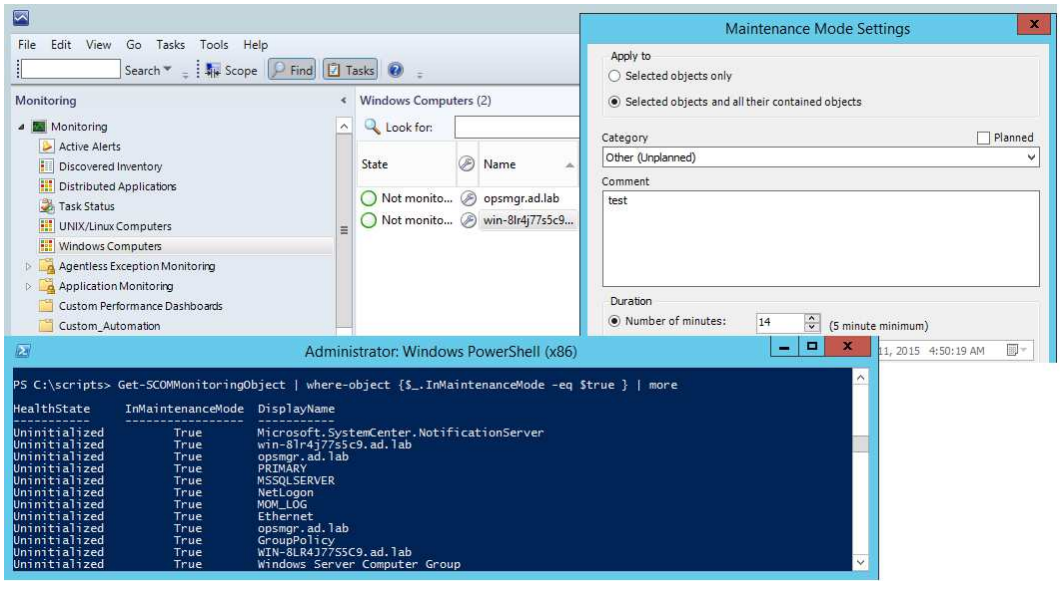
KUVIO 72. Windows Server 2012 R2 task scheduler: tehtävän asetukset

Seuraavaksi voidaan käynnistää testiä varten tehtävä valitsemalla sen kohdalta ”run”. Kuviosta 73. voidaan havaita, että tehtävä suoritettiin onnistuneesti.



KUVIO 73. Windows Server 2012 R2 task scheduler: tehtävän käynnistys

Tarkistetaan vielä lopuksi, että ryhmästä Windows Server Computer Group palvelimet menivät todellakin huoltotilaan. Tehtävän suorittamisen tarkistus, voidaan tehdä monella tapaa, esimerkiksi SCOM 2012 R2 hallintakonsolista tai varmistaa powershell-komentotulkin avulla (KUVIO 74). Palvelimet ovat menneet 15 minuutiksi huoltotilaan oikealla luokituksella ja kommentilla. Huoltotilan toteutumista voi myös tarkastella Windows-käyttöjärjestelmän omaa tapahtumalokia suodattamalla ja havaita sieltä tapahtuma toteutuneeksi (event id 1215).



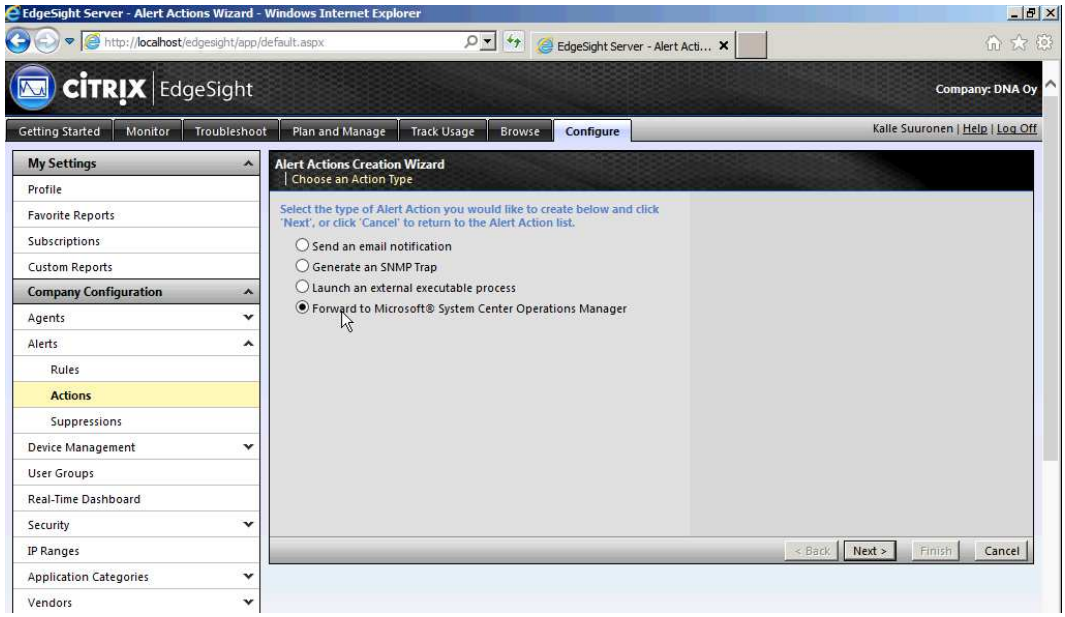
KUVIO 74. SCOM 2012 R2: ryhmä huoltotilassa

Microsoft Powershell -komentotulkin käyttö on erittäin suotavaa SCOM 2012 R2 -järjestelmän tehokkaassa hyödyntämisessä. Jos kaikki kohteet halutaan pois huoltotilasta samalla kertaa, voidaan se kätevästi toteuttaa powershell-komentosarjan avulla (liite 20).

7.12 SCOM 2012 R2- ja EdgeSight 5.4 –valvontajärjestelmien integraatio

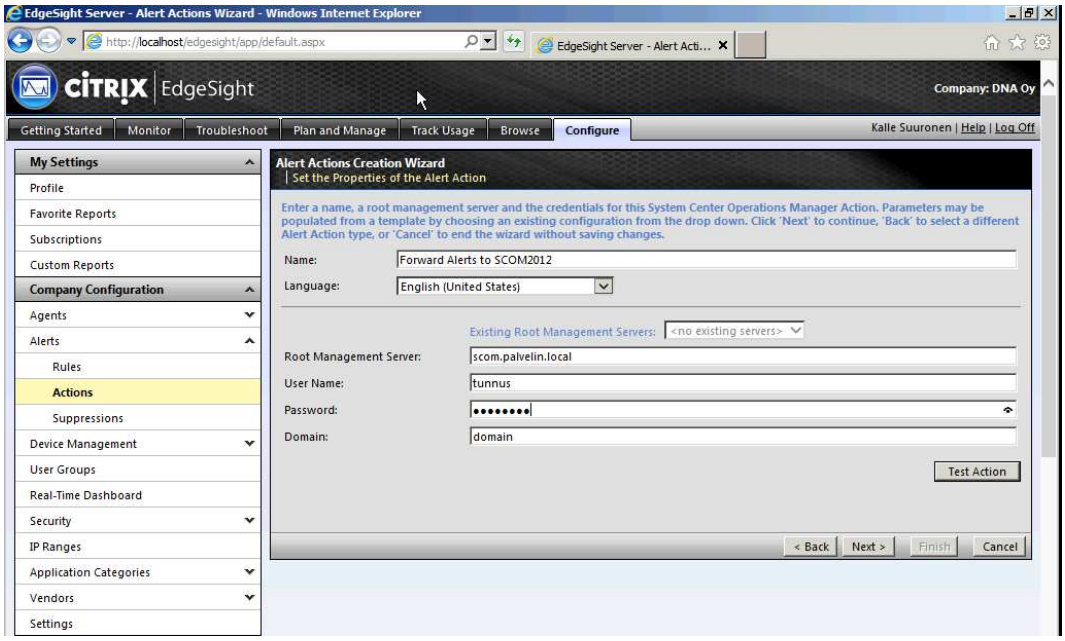
Integraatio valvontajärjestelmien välillä aloitetaan huolehtimalla, että Citrix.Library.mp- ja Citrix.PresentationServer.mp-hallintapaketit ovat asennettuna SCOM-hallintapalvelimelle. Kyseiset hallintapaketit tulevat vanhempien Citrix-tuotteiden mukana, mutta siirryttäessä uudempiin versioihin joudutaan hyödyntämään maksullisia hallintapaketteja. Citrix-palvelimilla täytyy olla myös asennettuna molempien valvontatyökalujen agentit ja EdgeSight-palvelimelle asennetaan vielä agenttien lisäksi Operations Manager Console. Citrix EdgeSight 5.4 median mukana tulee Citrix.EdgeSight.mp-hallintapaketti, joka otetaan käyttöön SCOM -palvelimella.

Kun kaikki pohjatyöt on saatu tehdyksi, EdgeSight-palvelin voidaan määritellä välittämään hälytysviestejä SCOM-palvelimelle. EdgeSight Server Console -konsolista avataan määritykset välilehti (configure), josta yrityksen määrityksistä (Company Configuration) avataan hälytykset (Alerts) ja toiminnot (Actions). Toimintojen alta luodaan uusi hälytystoiminto (New Alert Action), jolla viestit välitetään myös SCOM-palvelimelle (Forward to Microsoft System Center Operations Manager) (KUVIO 75).



KUVIO 75. Citrix EdgeSight 5.4: toiminnon tyypin valinta

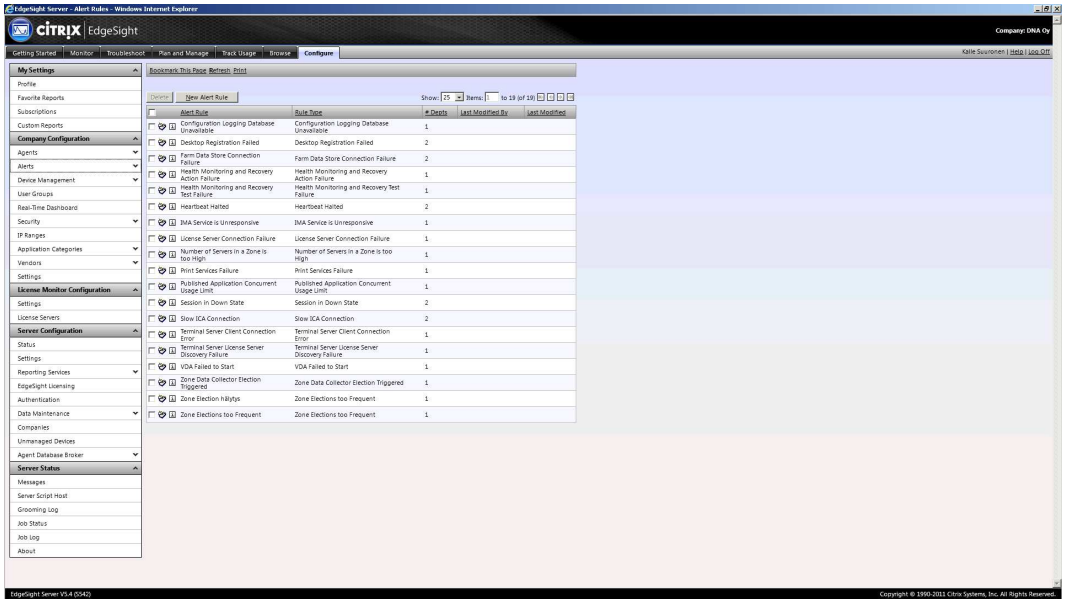
Määritetään seuraavaksi toiminnolle kuvaava nimi, SCOM-hallintapalvelimen FQDN tai IP-osoite, tarvittavat oikeudet omaava domain-tunnus ja käytettävä domain (KUVIO 76).



KUVIO 76. Citrix EdgeSight 5.4: toiminnon määritykset

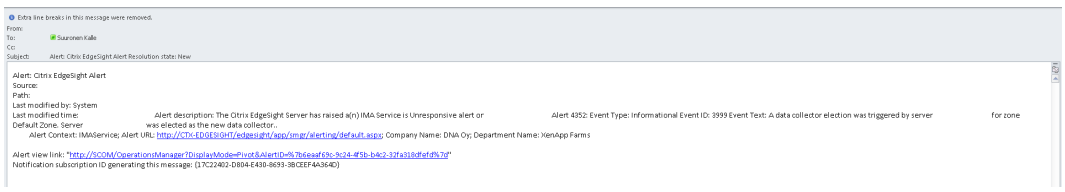
Luotu hälytystoiminto täytyy vielä liittää hälytyssääntöihin (alert rule) (KUVIO 77). Määritykset välilehden alta valitaan hälytykset ja säännöt ja käynnistetään Wizard. Valitaan seuraavaksi Change Alert Rule to Alert

Action Mappings, josta voidaan valita mihin osastoon viestien välittäminen halutaan yhdistää. Halutessaan voidaan esimerkiksi valita pelkästään XenApp- tai XenDesktop-palvelimet. Tässä tapauksessa halutaan valvoa kaikkia palvelimia ja clienttejä, joten valitaan kaikki. Sidotaan luotu toiminto sääntöön, joka tarkistaa, onko IMA-palvelu päällä palvelimella. Seuraavaksi voidaankin luoda vikatilanne ja testata, siirtyykö hälytys SCOM-hallintapalvelimelle ja siitä vielä eteenpäin luotua sähköpostikanavaa pitkin tilaajan sähköpostiin.



KUVIO 77. Citrix EdgeSight 5.4 -hälytyssäännöt

Testin lopuksi voidaan havaita, että Citrix EdgeSightin muodostama hälytys on viety SCOM-hallintapalvelimelle ja hälytyksestä on lähetetty sähköpostiin viesti (KUVIO 78).



KUVIO 78. SCOM 2012 R2:n ja EdgeSightin välittämänä hälytysviesti

8 YHTEENVETO

8.1 Työn tausta

Opinnäytetyön tavoitteena oli selvittää, kuinka Microsoft System Center Operations Manager ja Citrix EdgeSight -valvontajärjestelmiä voitaisiin hyödyntää Citrix-julkaisujärjestelmän valvonnassa. Työn teemana on vahvasti virtualisointi ja verkonvalvonta. Työssä käytiin läpi yleisiä virtualisointitapoja ja keskeisimpiä järjestelmiä Citrix-julkaisujärjestelmän kannalta syvennyttiin hieman niiden toimintaan. Työssä paneuduttiin myös EdgeSight 5.4- ja SCOM 2012 R2 -valvontajärjestelmiin sekä tärkeisiin verkonvalvontatekniikoihin: SNMP ja WMI, joita valvontajärjestelmät hyödyntävät toiminnassaan.

Käytännön toteutusta ja kartoitusta tehtiin ensin yrityksen omassa ympäristössä, josta käytännön osuus jatkui omassa virtuaalisessa testiympäristössä. Oma testiympäristö sisälsi Microsoft System Center Operations Manager-, SQL-, AD- ja DNS-virtuaalipalvelimen. Yrityksessä oli lähtötilanteessa valmiina Citrix EdgeSight 5.4 -valvontajärjestelmä ja siihen tehdyt perusmääritykset. Järjestelmään liittyvät valvonta-agentit olivat myös asennettuina. Työ käsitteleekin käytännön osalta lähes kokonaan Microsoft System Center Operations Manager 2012 R2 -valvontajärjestelmän käyttöönottoa ja siihen liittyviä tärkeimpiä perusmäärityksiä opiskelijan näkökulmasta. Tehty käytännön työ ja määritykset toimivat ohjeistavina, jolloin niitä voidaan helposti soveltaa Citrix-julkaisujärjestelmän valvonnassa tai hyödyntää jonkin muun ympäristön valvontaan.

8.2 Citrix-julkaisujärjestelmä

Citrix-julkaisujärjestelmä voidaan mieltää yhtenä suurena kokonaisuutena, joka koostuu useasta erilaisesta järjestelmästä. Julkaisujärjestelmän keskiössä toimivat sovellusvirtualisointiin tarkoitettu Citrix XenApp ja Microsoft App-V sekä työpöytävirtualisointiin tarkoitettu Citrix XenDesktop. Citrix-julkaisujärjestelmän tehtävänä on tarjota tietoturvallisesti ja

vaivattomasti käyttäjille käyttöjärjestelmästä, laitteesta tai paikasta riippumattomia virtualisoituja sovelluksia ja virtuaalityöpöytiä.

Käyttäjän näkökulmasta Citrix-julkaisujärjestelmä ilmenee kaikessa yksinkertaisuudessaan WWW-sivustona, jonne käyttäjä kirjautuu omilla tunnuksillaan. Kun käyttäjä on kirjautunut sivustoon, hänelle voidaan tarjota pääsyä erilaisiin resursseihin keskitetysti: virtualisoituihin sovelluksiin, tiedostoihin, hakemistoihin tai virtuaalityöpöytään. Käyttäjä tarvitsee Citrix Receiver -asiakasohjelman ja WWW-selaimen, jotta hän pystyy hyödyntämään virtualisoituja resursseja. Käyttäjälle osoitetut resurssit tuodaan hänen ulottuville kuvainformaationa.

8.3 Valvontajärjestelmien roolit ja toteutuksen valinta

Hyödynnettävinä valvontajärjestelminä olivat Citrix EdgeSight 5.4 ja Microsoft System Center Operations Manager 2012 R2. Valvontajärjestelmien toimintaa kartoitettiin teoriassa ja käytännössä miettien niiden heikkouksia ja vahvuuksia. Citrix EdgeSight 5.4:n vahvuudet ovat erityisesti Citrix XenApp- ja XenDesktop-järjestelmien valvonnassa ja käyttäjäkokemuksen mittaamisessa. SCOM 2012 R2 mahdollistaa kattavan infrastruktuurin valvonnan, automaation ja hyvän muokattavuuden. Hallintapakettiensa ansiosta SCOM 2012 R2 -valvontajärjestelmällä pystytään valvomaan kattavasti muita Citrix-julkaisujärjestelmään kuuluvia järjestelmiä ja niiden toimintaa.

Suosituksena valvonnan toteuttamiselle olisi yhdistää Citrix EdgeSight- ja SCOM 2012 R2 -valvontajärjestelmien toiminta keskittäen hälytystenkäsittelyn täysin SCOM 2012 R2:n alle. SCOM 2012 R2 -valvontajärjestelmää käytettäisiin koko Citrix-julkaisujärjestelmän valvonnassa keskitetysti valvonnassa, diagnosoinnissa ja automatisoinnissa. Citrix EdgeSight -valvontajärjestelmää hyödynnettäisiin laajemmin silloin, kun tarvitaan tarkkaa tietoa ICA-istunnoista ja Citrix-palveluiden saatavuudesta. Raportoinnin osalta Citrix EdgeSight tarjoaa tarvittavat raportit Citrix-järjestelmien osalta ja SCOM 2012 R2 muiden järjestelmien.

8.4 Suositukset käytäntöön

Kun SCOM 2012 R2 -järjestelmää asennetaan (liite 4), huomioidaan muutama tärkeä asia. Laitteistovaatimuksia varten suositellaan käytettäväksi SCOM 2012 Sizing Helper Tool -ohjelmaa, jolla voidaan helposti saada selville tarvittavat laitteistovaatimukset perustuen parhaisiin käytäntöihin. Tietoturvanäkökulmasta käytössä pitäisi olla SSL-salaus, jota varten luodaan ja jaetaan avaimet. Salaus on pääsääntöisesti SCOM 2012 R2 -selaimella hyödynnettävää hallintakonsolia (liite 12) ja raportointia varten (liite 11). SCOM 2012 R2 hyödyntää neljää domain-palvelutunnusta toiminnassaan. Jokaista tunnusta kohti tulisi luoda käyttötarkoitusta vastaavilla oikeuksilla oleva tunnus (liite 4). Domain tunnuksia hyödynnettäessä tulee netbios- ja FQDN-nimi rekisteröidä.

SCOM 2012 R2:n asennuksen jälkeen tulisi olla viimeistään selvillä, mitä kohteita eli palvelimia ja laitteita valvotaan. Sen jälkeen kartoitetaan tarkemmin valvottavien kohteiden sisältämät ohjelmat, toiminnot ja palvelut. Kaikkiin Citrix-julkaisujärjestelmän järjestelmiin löytynee omat hallintapaketit, joiden avulla saadaan käyttöön tuotteen valmistajan luomat parhaat käytännöt valvonnan osalta. Citrix tarjoaa dokumentin (liitetiedosto Operations Guide – Monitoring.pdf), jota hyödyntäen voidaan helposti tunnistaa valvottavat komponentit, suorituskykylaskurit ja tapahtumat.

Kartoituksen jälkeen asennetaan Microsoft Monitoring Agent valvottaviin kohteisiin (liite 5) ja aloitetaan hallintapakettien asennus (liite 6). Hallintapakettien asennus aloitetaan asentamalla yksitellen hallintapaketit ja lisäämällä valvottavat kohteet manuaalisesti valvottaviksi. Hallintapakettien asennus tulisi aloittaa ensin SCOM 2012 R2 –järjestelmää tukevien järjestelmien ympäriltä, jotta itse valvontajärjestelmä saataisiin ensin kuntoon. Seuraavaksi seulotaan läpi kaikki virheelliset hälytykset, epäolennainen tieto ja mahdolliset virheelliset kynnysarvot. Käytetään epäollennaisen informaation suodatukseen override-toimintoa (liite 9). Muutokset tulisi tallentaa aina itse luotuihin avoimiin hallintapaketteihin. Riippuen hallintapakettiin liittyvien valvottavien kohteiden määrästä, olisi hallintapakettien asentamisen välillä pitää taukoa

muutama päivä. Jos hallintapaketteja asennetaan useita samalla, tiedon määrä voi lisääntyä dramaattisesti ja tiedon suodattaminen vaikeutua huomattavasti. Huoltotilaa hyödyntämällä (liite 15) voidaan myös karsia turhia hälytyksiä, jos yrityksessä esimerkiksi käynnistetään päivityksiä tai huoltoa varten säännöllisesti palvelimia.

Jotta Citrix-julkaisujärjestelmää voidaan valvoa kattavasti, otetaan SCOM 2012 R2 -järjestelmän ohelle EdgeSight 5.4 käyttöön. Asennetaan tarvittavat hallintapaketit ja ohjelmat sekä määritetään EdgeSight 5.4 -valvontajärjestelmä välittämään hälytysviestit SCOM 2012 R2 -valvontajärjestelmälle (liite 17). Nyt pääasiallinen hälytystenvalvonta voidaan toteuttaa keskitetysti SCOM 2012 - Operations Consolen kautta. SCOM 2012 R2 -järjestelmästä määritetään integroinnin jälkeen hälytysviestien välittäminen sähköpostiin (liite 8), jolloin vikatilanteisiin pystytään reagoimaan nopeammin.

Tehokkaassa SCOM 2012 R2:n hyödyntämisessä olisi hyvä hyödyntää mukautettuja ryhmiä: dynaamisia (liite 7) tai staattisia. Mukautetuilla ryhmillä saadaan luotua ryhmä omia valittuja kohteita eri ryhmistä yhdeksi kokonaisuudeksi. Mukautettujen ryhmien ohella luodaan omia näkymiä, jossa voidaan hyödyntää mukautettuja ryhmiä. Omilla näkymillä on mahdollista saada suodatettua näkyviin vain itselle tärkein tieto (liite 13) tai vaihtoehtoisesti luoda toisille SCOM-käyttäjille (liite 10) näkymiä jakamaan tarvittavaa tietoa, esimerkiksi HelpDeskille palvelimien tilasta. Jos valvontajärjestelmällä on useita muita käyttäjiä, tulisi heille luoda omat SCOM-käyttäjätunnukset rajaten oikeudet heidän tarpeensa mukaan (liite 10). Esimerkiksi pelkkää historiallista raportointia (liite 11) varten tulisi luoda omat tunnukset. Tehokkaaseen valvontajärjestelmän hyödyntämiseen kuuluu myös automatisointi. Kun useimmin toistuvia hälytyksiä seurataan voidaan, esimerkiksi havaita tiettyjen palveluiden toiminnan lakkaaminen. SCOM 2012 R2:n avulla voidaan näistä vikatilanteista palautua automaattisesti (liite 14). Varmuuskopioiden ottaminen on ehdottoman tärkeää mahdollisten valvontajärjestelmän vikatilanteiden varalle. SCOM 2012 R2 -tietokannoista ja avoimista hallintapaketeista tulisi ottaa varmuuskopiot säännöllisin väliajoin (liite 19).

9 JOHTOPÄÄTÖKSET

Tämän työn tavoitteena oli olla ohjeistavana työnä DNA Oy:n Citrix-julkaisujärjestelmän valvonnalle ja toteuttamiselle hyödyntämällä Citrix EgeSight- ja Microsoft System Center Operations Manager -valvontajärjestelmiä. Kun SCOM 2012 R2 -valvontajärjestelmään tehtiin määrityksiä tuli nopeasti selville, että saatavilla olevia Citrix-hallintapaketteja ei voitu hyödyntää niiden ollessa vanhentuneita nykyisiin versioihin nähden. Toteutuksen valinnaksi muodostui molempien valvontajärjestelmien hyödyntäminen keskittämällä hälytysten käsittely SCOM 2012 -valvontajärjestelmään. Molempia järjestelmiä hyödyntämällä pystytään kattamaan valvonta koko Citrix-julkaisujärjestelmän osalta. Muussa tapauksessa osa järjestelmistä jäisi täysin ilman valvontaa.

Työn laajuuden vuoksi ja jo käyttöönotetun Citrix EdgeSight 5.4 -valvontajärjestelmän myötä käytännön työn määritykset painottuivat SCOM 2012 R2:n ympärille. Tehdyt määritykset luotiin ohjeistaviksi, jolloin niitä voidaan myös soveltaa tulevaisuudessa muissakin järjestelmissä. Määrityksissä pyrittiin huomioimaan asioita mahdollisimman laajasti, mutta yksinkertaisesti. Kaikki tehdyt määritykset testattiin onnistuneesti. Ohjeita soveltamalla voidaan SCOM 2012 R2 -valvontajärjestelmää hyödyntää tehokkaasti Citrix-julkaisujärjestelmän valvonnassa. Tehokas SCOM 2012 R2:n hyödyntäminen vaatii jatkuvaa valvontaympäristön muokkaamista, joka muiden töiden ohella vie ajallisesti paljon resursseja.

Tulevaisuudessa olisi hyvä pohtia mahdollisesti uudempien versioiden Citrix-hallintapakettien hankkimista SCOM 2012 R2 -valvontajärjestelmälle. Hallintapaketit mahdollistaisivat samat valvonta-mahdollisuudet SCOM 2012 -valvontajärjestelmässä kuin EdgeSight nyt tarjoaa. Citrix-julkaisujärjestelmää voitaisiin valvoa kokonaisvaltaisemmin yhden valvontajärjestelmän kautta ja valvontajärjestelmää tarvitsisi muokata huomattavasti vähemmän, joka vähentäisi ylläpitotehtäviä valvonnan osalta. Citrix suosittaakin yhden valvontajärjestelmän käyttöä järjestelmiensä ja kokonaisuuksien valvonnassa.

LÄHTEET

Allied Telesis. 2015. Simple Network Management Protocol (SNMP) [viitattu 14.5.2015]. Saatavissa: http://www.alliedtelesis.com/media/fount/software_reference/271/ar400/snmp.pdf

Brennan, M., Briggs, R., Shbeilat, L. & Anderson, F. 2012. Citrix XenDesktop on FlexPod with Microsoft Private Cloud [viitattu 14.5.2015]. Saatavissa: http://www.cisco.com/en/US/docs/unified_computing/ucs/UCS_CVDs/ucs_xd56_flexpod.html

Bunn, F., Simpson, N., Peglar, R. & Nagle, G. 2010. Storage Virtualization. SNIA Technical Tutorial [viitattu 14.5.2015]. Saatavissa: http://www.snia.org/sites/default/files/sniavirt.pdf

Cisco Systems, Inc. 2009. Network Virtualization—Path Isolation Design Guide [viitattu 14.5.2015.]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html

Cisco Systems, Inc. 2012. Simple Network Management Protocol [viitattu 14.5.2015]. Saatavissa: http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol#SNMP_Basic_Commands

Citrix Systems, Inc. 2007. Citrix EdgeSight for Presentation Server [viitattu 14.5.2015]. Saatavissa: http://www.preferredtechnology.com/files/Citrix%20EdgeSight%20for%20Presentation%20Server.pdf

Citrix Systems, Inc. 2010a. Citrix EdgeSight Administrator's Guide [viitattu 14.5.2015]. Saatavissa: http://support.citrix.com/servlet/KbServlet/download/23021-102-666025/EdgeSight_Admin_Guide.pdf

Citrix Systems, Inc. 2010b. XenDesktop 5 Reference Architecture [viitattu 14.5.2015]. Saatavissa: http://support.citrix.com/servlet/KbServlet/download/25558-102-648748/Reference%20Architecture%20-%20XenDesktop%205.pdf

Citrix Systems, Inc. 2011a. Citrix EdgeSight User's Guide [viitattu 14.5.2015]. Saatavissa: https://support.citrix.com/servlet/KbServlet/download/28276-102-666246/EdgeSight_User_Guide.pdf

Citrix Systems, Inc. 2011b. Scaling Big – DaaS and SaaS Deployments for Citrix Service Providers [viitattu 14.5.2015]. Saatavissa: http://support.citrix.com/servlet/KbServlet/download/26876-102-671606/ScalingBig%20-%20DaaS%20SaaS%20deployments%20for%20Citrix%20Service%20Providers_1108.pdf

Citrix Systems, Inc. 2013. Map client devices [viitattu 14.5.2015]. Saatavissa: http://support.citrix.com/proddocs/topic/receiver-windows-40/ica-mapping-client-devices-v2.html

Citrix Systems, Inc. 2014a. Citrix ICA Virtual Channels Backgrounder [viitattu 14.5.2015]. Saatavissa: http://support.citrix.com/article/CTX116890

Citrix Systems, Inc. 2014b. Citrix HDX technologies for optimizing the virtualization experience [viitattu 14.5.2015]. Saatavissa: http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-hdx-technologies.pdf

Citrix Systems, Inc. 2015a. About EdgeSight [viitattu: 14.5.2015]. Saatavissa: http://support.citrix.com/proddocs/topic/edgesight54/es-about-wrapper.html

Citrix Systems, Inc. 2015b. About Us [viitattu 14.5.2015]. Saatavissa: http://www.citrix.com/about.html

Citrix Systems, Inc. 2015c. EdgeSight End User Experience Monitoring Statistics Explained [viitattu 14.5.2015]. Saatavissa: http://support.citrix.com/article/CTX114495

Citrix Systems, Inc. 2015d. Session virtualization and app virtualization with XenApp [viitattu 14.5.2015]. Saatavissa: http://www.citrix.com/products/xenapp/how-it-works/application-virtualization.html

De Luca, A. & Bhide, M. 2010. Storage Virtualization for dummies – Hitachi Data Systems Edition. Indianapolis: Wiley Publishing Inc. [viitattu 14.5.2015]. Saatavissa: http://www.hds.com/assets/pdf/hitachi-data-systems-storage-virtualization-for-dummies-nl.pdf

Fujitsu. 2011. White paper VDI Reference Architecture for Citrix XenDesktop and Fujitsu PRIMERGY BX900 [viitattu 14.5.2015]. Saatavissa: http://globalsp.ts.fujitsu.com/dmsp/Publications/public/wp-vdi-refarch-xd-bx900.pdf

Golden B. & Scheffy C. 2008. Virtualization For Dummies, Sun and AMD Special Edition. Indiana: Wiley Publishing Inc. [viitattu 14.5.2015]. Saatavissa: http://www.cardsictsolutions.nl/upload/resources/pdf/virtualization-for-dummies-5344.pdf

Golden, B. 2011. Virtualization for dummies. 3. uudistettu painos Hewlett-Packard Special Edition. Indianapolis: Wiley Publishing Inc. [viitattu 14.5.2015]. Saatavissa: https://ssl.www8.hp.com/de/de/pdf/virtuallisation_tcm_144_1147500.pdf

Harder, J. & Maynard, J. 2015. Technical Deep Dive: ICA Protocol and Acceleration [viitattu 14.5.2015]. Saatavissa: http://s3.amazonaws.com/legacy.icmp/additional/ica_acceleration_0709a.pdf

Intel. 2015. Intel Virtualization Technology [viitattu 14.5.2015]. Saatavissa: http://www.intel.com/content/www/us/en/virtualization/virtualization-technology/hardware-assist-virtualization-technology.html

ManageEngine. 2015. SNMP tutorial [viitattu 14.5.2015]. Saatavissa: http://www.manageengine.com/network-monitoring/what-is-snmp.html#snmp-version

Mauro, D. & Schmidt, K. 2005. Essential SNMP, Second Edition. Sebastopol: O'Reilly Media, Inc.

Microsoft. 2010. Overview of Application Virtualization [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/ee958112.aspx

Microsoft. 2011. Infrastructure Planning and Design Microsoft Application Virtualization 4.6 [viitattu 14.5.2015]. Saatavissa: https://msdn.microsoft.com/en-us/library/ee354207.aspx

Microsoft. 2013a. Comparing the Operations Console and Web Console in Operations Manager [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-US/library/hh230724.aspx

Microsoft. 2013b. Dependency Monitors [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/hh457606.aspx

Microsoft. 2013c. How Heartbeats Work in Operations Manager [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/library/hh212798.aspx

Microsoft. 2013d. Managing Run As Accounts and Profiles [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/hh212714.aspx

Microsoft. 2013e. Monitors and Rules [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/hh457603.aspx

Microsoft. 2013f. Operations Guide for System Center 2012 – Operations Manager [viitattu 16.5.2015]. Saatavissa: https://www.microsoft.com/en-us/download/confirmation.aspx?id=29256

Microsoft. 2013g. Operations Manager Key Concepts [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/hh230741.aspx

Microsoft. 2013h. Selecting a target [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/hh457539.aspx#WhereMonitorWillRun

Microsoft. 2013i. Supporting Infrastructure [viitattu 14.5.2015]. Saatavissa: https://technet.microsoft.com/en-us/library/hh487285.aspx

Microsoft. 2013j. Understanding Classes and Objects [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/hh457568.aspx#Class

Microsoft. 2013k. View Types In Operations Manager [viitattu 16.5.2015]. Saatavissa: https://technet.microsoft.com/en-us/library/hh230762.aspx

Microsoft. 2013l. What Is in an Operations Manager Management Pack [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/hh212794.aspx

Microsoft. 2014. Getting Started With App-V 5.0 [viitattu 14.5.2015]. Saatavissa: https://technet.microsoft.com/en-us/library/jj713418.aspx

Microsoft. 2015a. About Performance Counters [viitattu 14.5.2015]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/desktop/aa371643(v=vs.85).aspx

Microsoft. 2015b. Application Virtualization (App-V) [viitattu 14.5.2015]. Saatavissa: http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/mdop/app-v.aspx

Microsoft. 2015c. Hardware Management Introduction [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/cc785056(v=ws.10).aspx

Microsoft. 2015d. Performance Counters [viitattu 14.5.2015]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/desktop/aa373083(v=vs.85).aspx

Microsoft. 2015e. WMI Architecture [viitattu 14.5.2015]. Saatavissa: http://msdn.microsoft.com/en-us/library/aa394553(v=vs.85).aspx

Microsoft. 2015f. WMI Infrastructure [viitattu 14.5.2015]. Saatavissa: https://msdn.microsoft.com/en-us/library/aa394562%28v=vs.85%29.aspx

Microsoft. 2015g. Windows Management Instrumentation and Simple Network Management Protocol [viitattu 14.5.2015]. Saatavissa: http://technet.microsoft.com/en-us/library/bb742612.aspx#EDAA

Microsoft. 2015h. Windows Remote Management [viitattu 14.5.2015]. Saatavissa: http://msdn.microsoft.com/en-us/library/aa384426(v=vs.85).aspx

Morgan, A. 2015. Decrapifying the Citrix Web Interface (5.4) [viitattu 30.5]. Saatavissa: http://andrewmorgan.ie/2011/08/decrapifying-the-citrix-web-interface-5-4

Musumeci, G. 2012. Getting Started with Citrix XenApp 6.5. Birmingham: Packt Publishing Ltd.

Ramlal, K. & Card, T. 2006. Independent Management Architecture Internals [viitattu 14.5.2015]. Saatavissa: http://www.slideshare.net/albertspijkers/independent-management-architecture-internals. Asiantuntijaluento Citrix Forum 2006.

Savill, J. 2012. Microsoft Virtualization Secrets. Indianapolis: John Wiley & Sons, Inc.

SevOne, Inc. 2015. The Benefits of Network Performance Monitoring and Management [viitattu 14.5.2015]. Saatavissa: http://www.sevone.com/technologies/performance-monitoring-benefits

Shabaz. 2014. Citrix XenApp 6.5 Architectural Components. [viitattu 31.5.2015]. Saatavissa: http://shabaztech.com/citrix-xenapp-6-5-architectural-components

Vmware. 2006. Virtualization Overview [viitattu 14.5.2015]. Saatavissa: https://www.vmware.com/pdf/virtualization.pdf

Vmware. 2007. Vmware Virtual Networking Concepts [viitattu 14.5.2015]. Saatavissa: https://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

Wikipedia. 2014. Independent Computing Architecture [viitattu 14.5.2015]. Saatavissa: http://en.wikipedia.org/wiki/Independent_Computing_Architecture

Wikipedia. 2015a. Application Virtualization [viitattu 14.5.2015]. Saatavissa: http://en.wikipedia.org/wiki/Application_virtualization

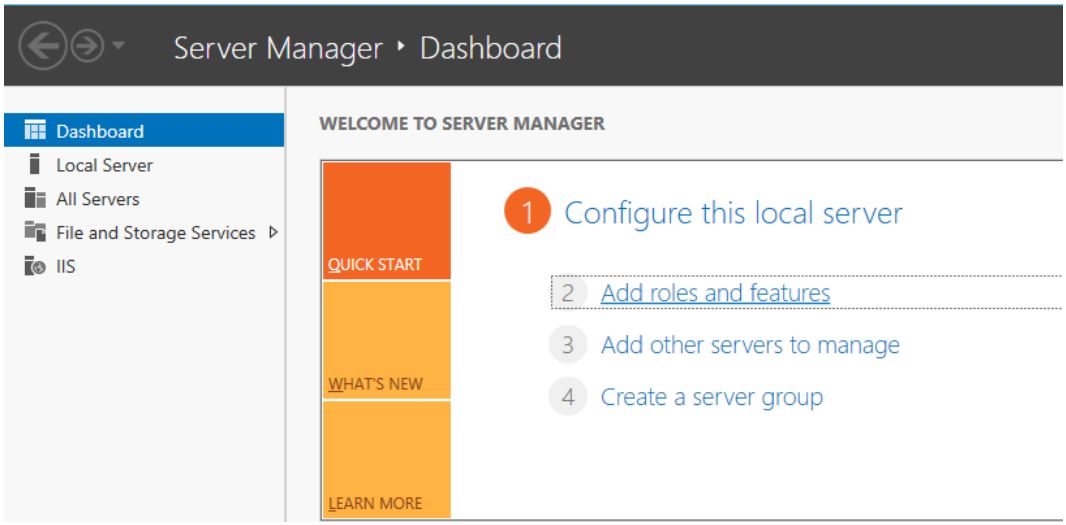
Wikipedia. 2015b. Desktop virtualization [viitattu 14.5.2015]. Saatavissa: http://en.wikipedia.org/wiki/Desktop_virtualization

Wikipedia. 2015c. Operating-system-level virtualization [viitattu 14.5.2015]. Saatavissa: http://en.wikipedia.org/wiki/Operating_system%E2%80%93level_virtualization

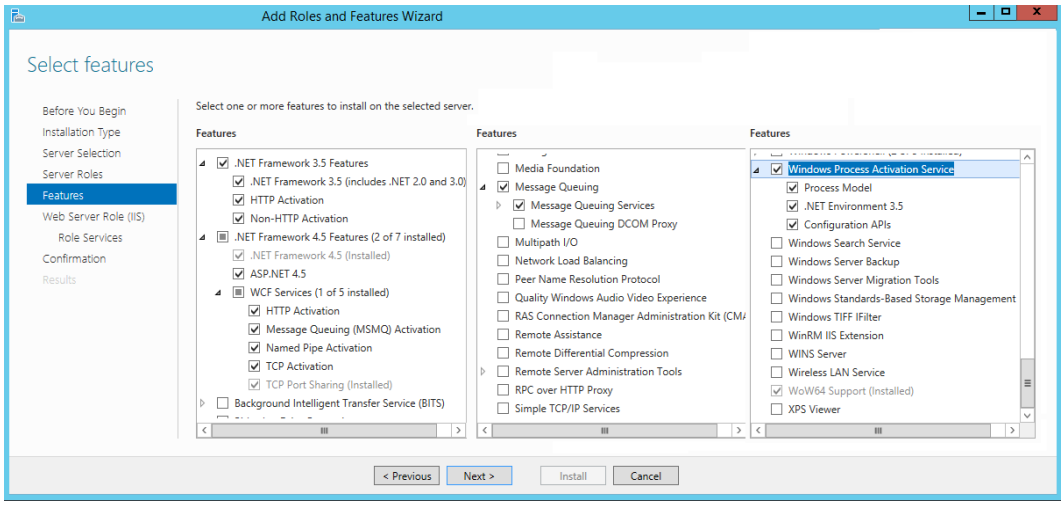
LIITTEET

Liite 1. SCOM 2012 R2 -testiympäristön valmistelu

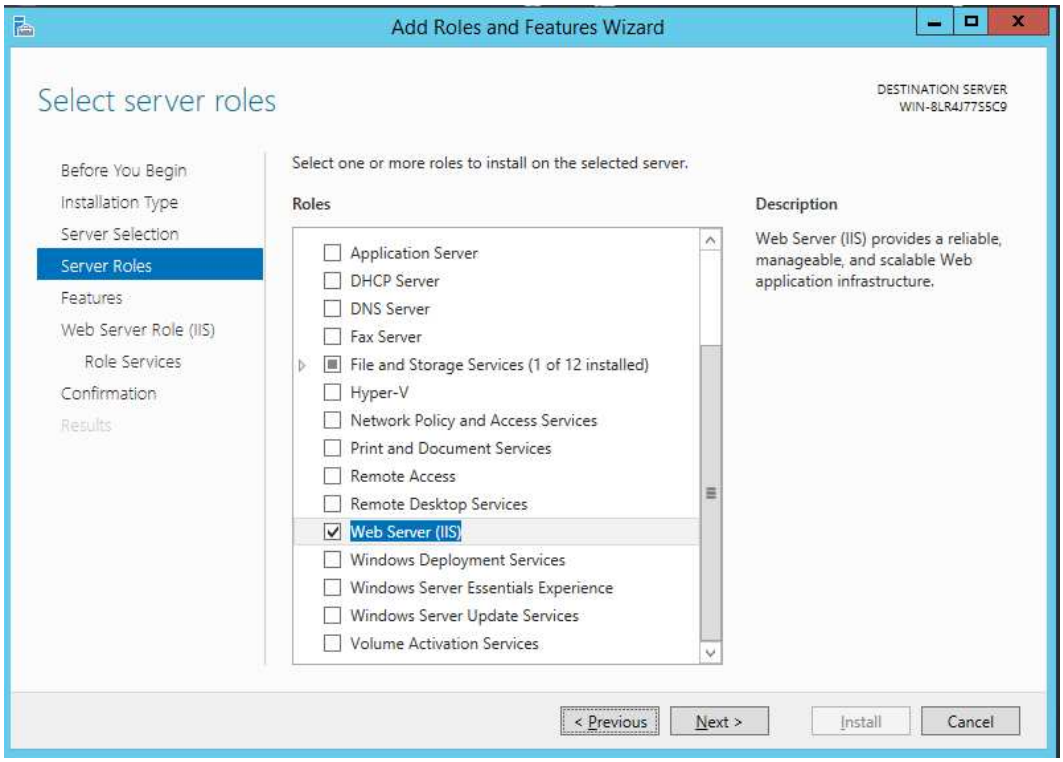
1. Valitaan palvelinhallinnassa Add roles and features.



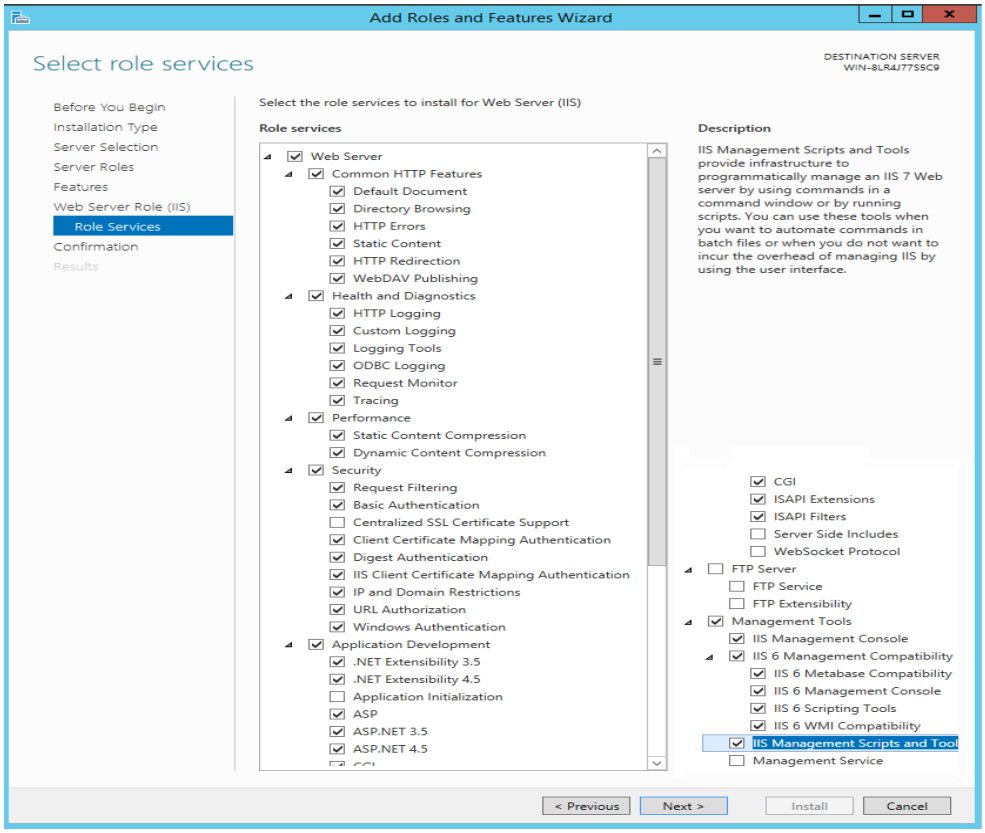
2. Valitaan SCOM asennukseen vaadittavat .NET 4.5 toiminnot.



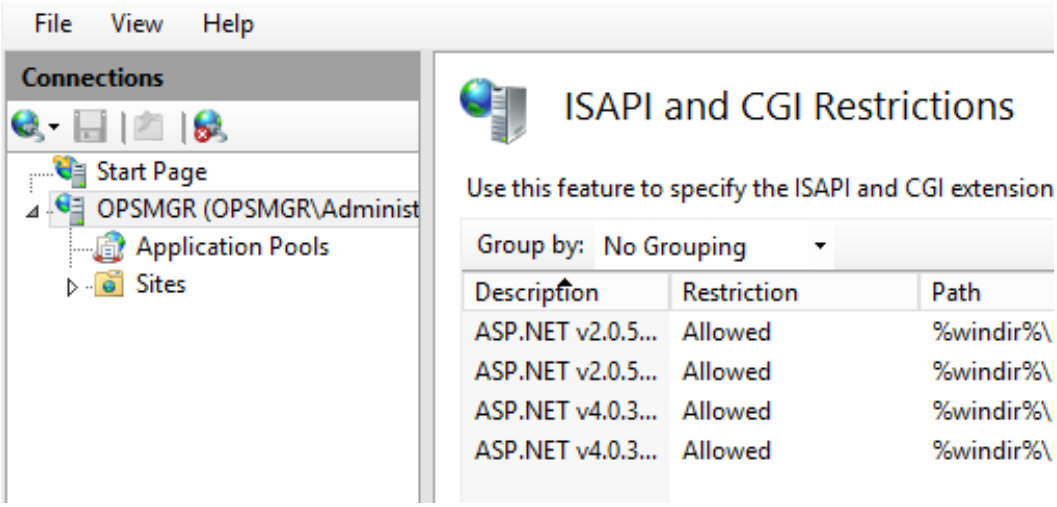
3. Kun .NET 4.5 kehys ja toiminnot ovat onnistuneesti asennettuna voidaan aloittaa Web Server (IIS) asennus. Valitaan Server Roles kohdasta Web Server (IIS) asennettavaksi.



4. Valitaan Web Server Role (IIS) kohdasta kaikki tarpeelliset palvelut SCOM varten.

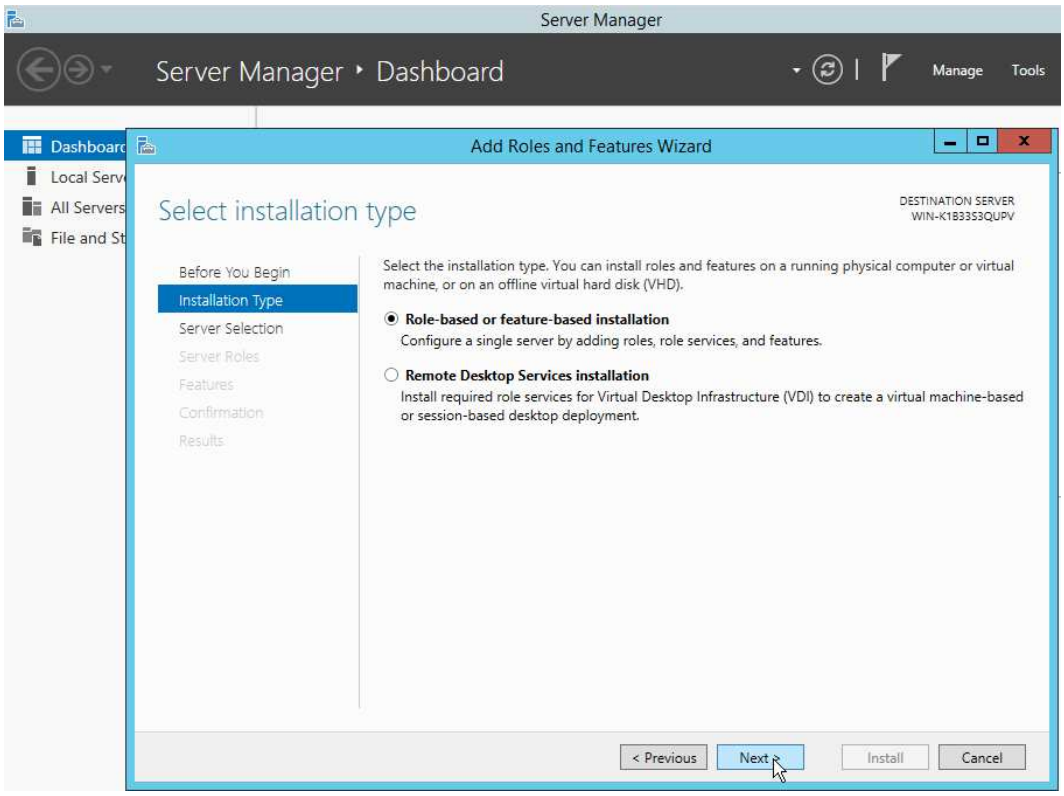


5. Käynnistetään Internet Information Server (IIS) Manager ja varmistetaan Web Consolea varten, että kohdasta ISAPI and CGI restrictions ASP.NET v.4.x on sallittuna.

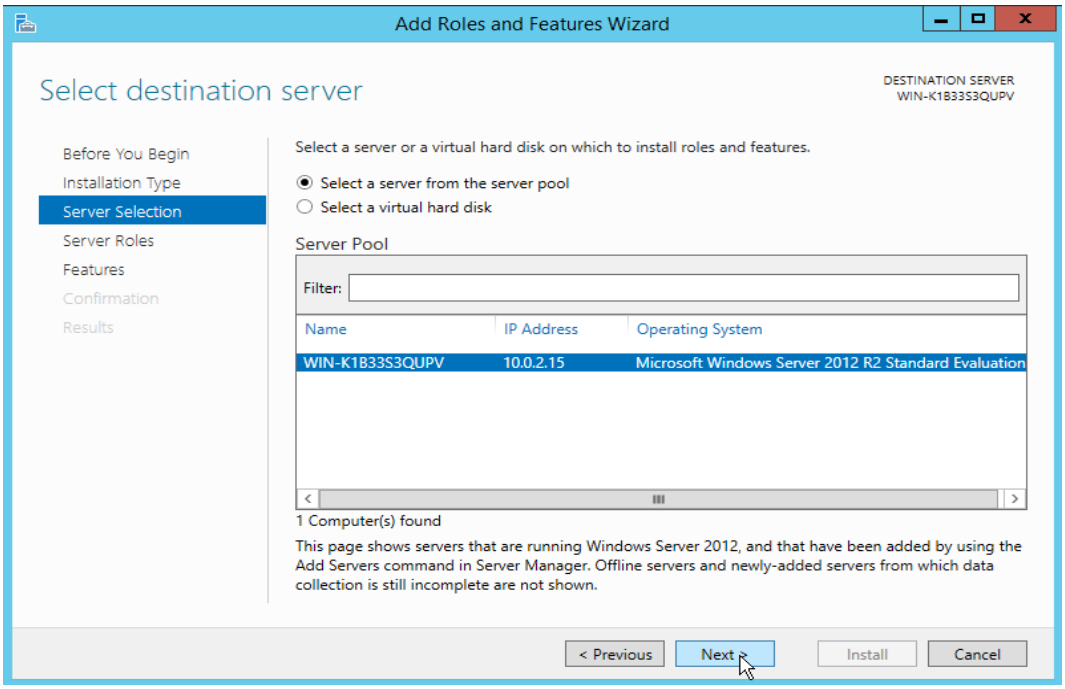


Liite 2. Active Directory- ja DNS-palvelimen asennus

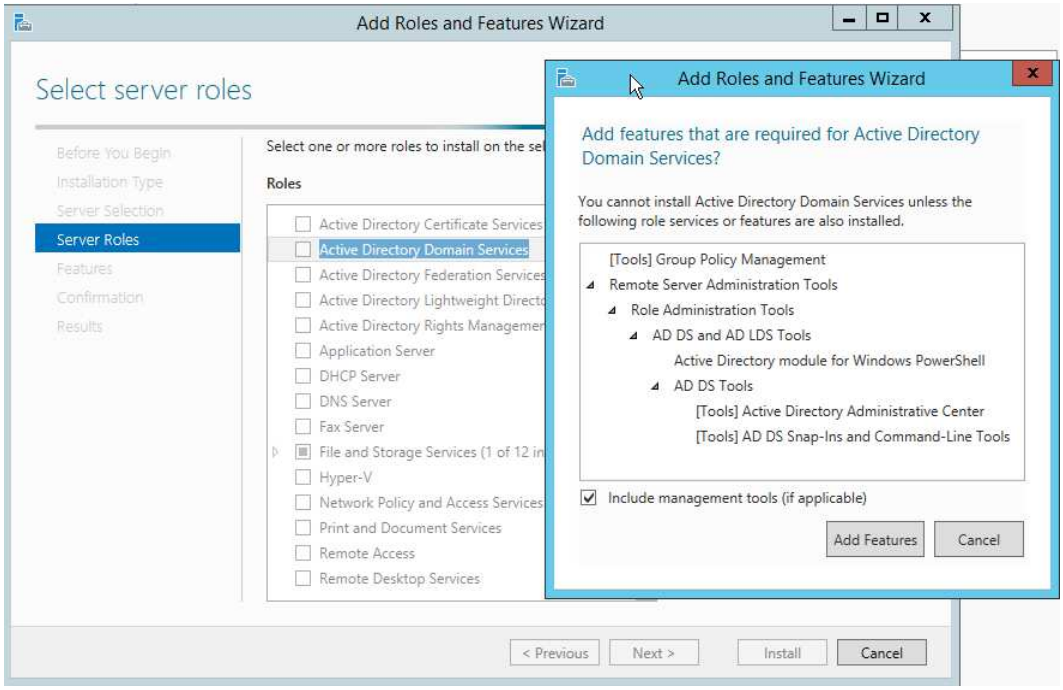
1. Valitaan palvelimen hallinnasta Add roles and features ja valitaan rooli asennettavaksi palvelimelle.



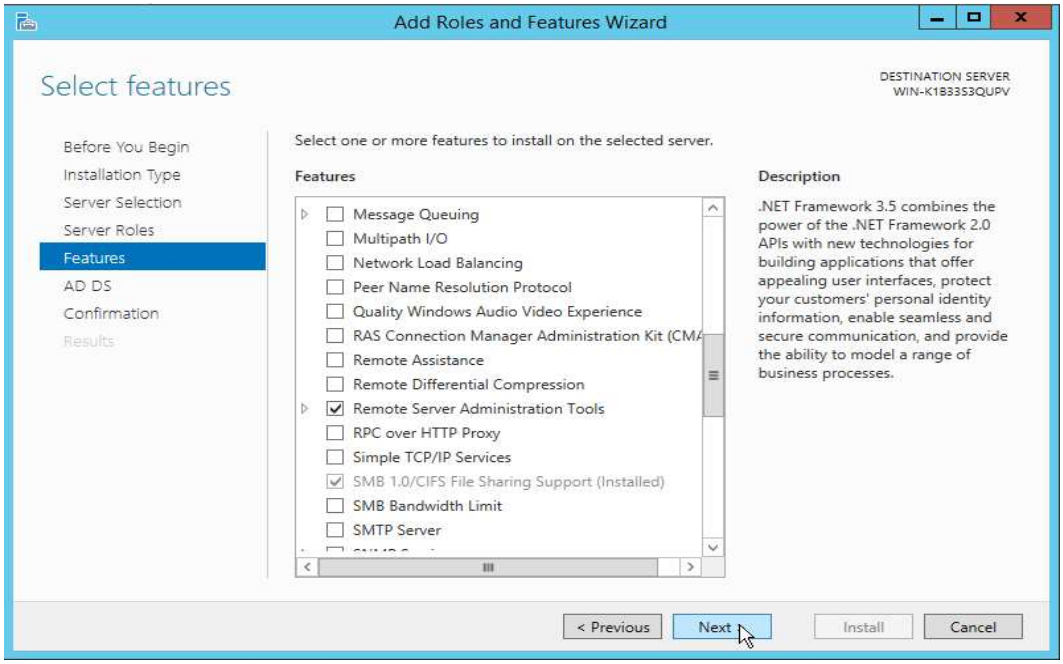
2. Valitaan Active Directoryn ja DNS -palvelimeksi paikallinen palvelin.



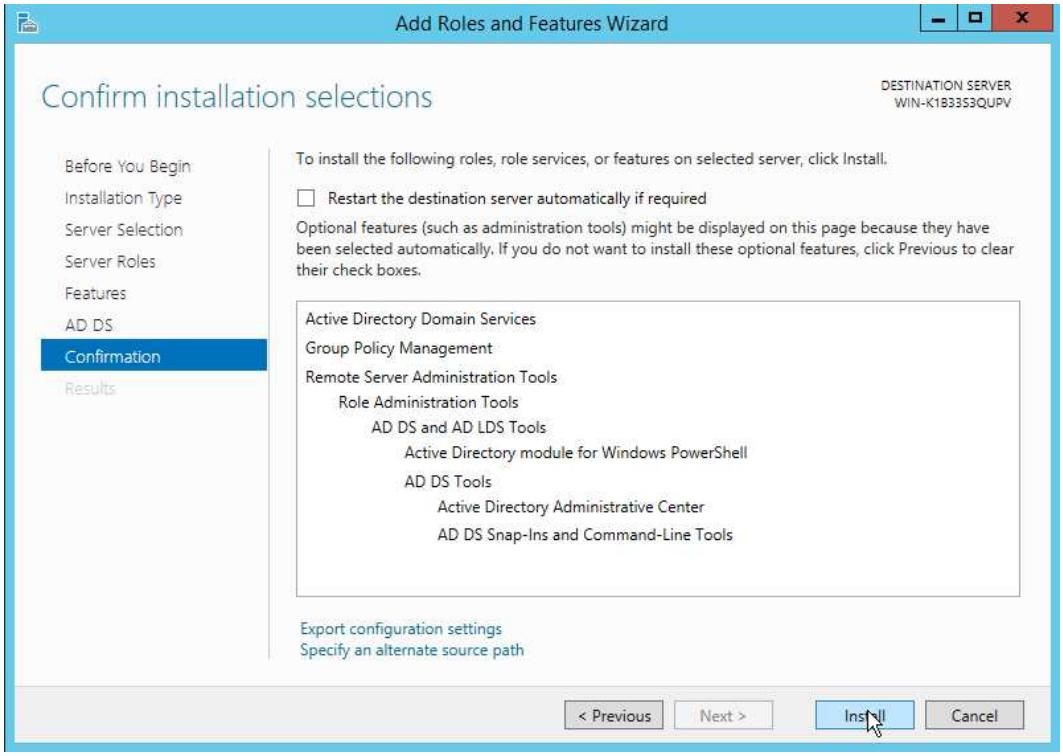
3. Valitaan asennettavaksi Active Directory Domain Services -rooli ja sen mukana tulevat toiminnot. DNS-roolia ei tarvi erikseen valita.



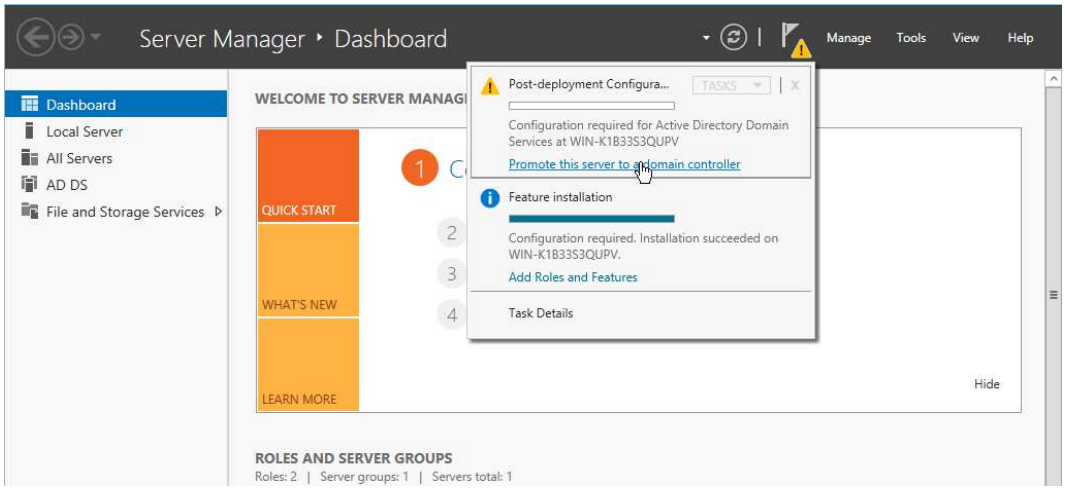
4. Seuraavaksi voidaan halutessa asentaa palvelimelle erilaisia toimintoja, jos niille on tarvetta.



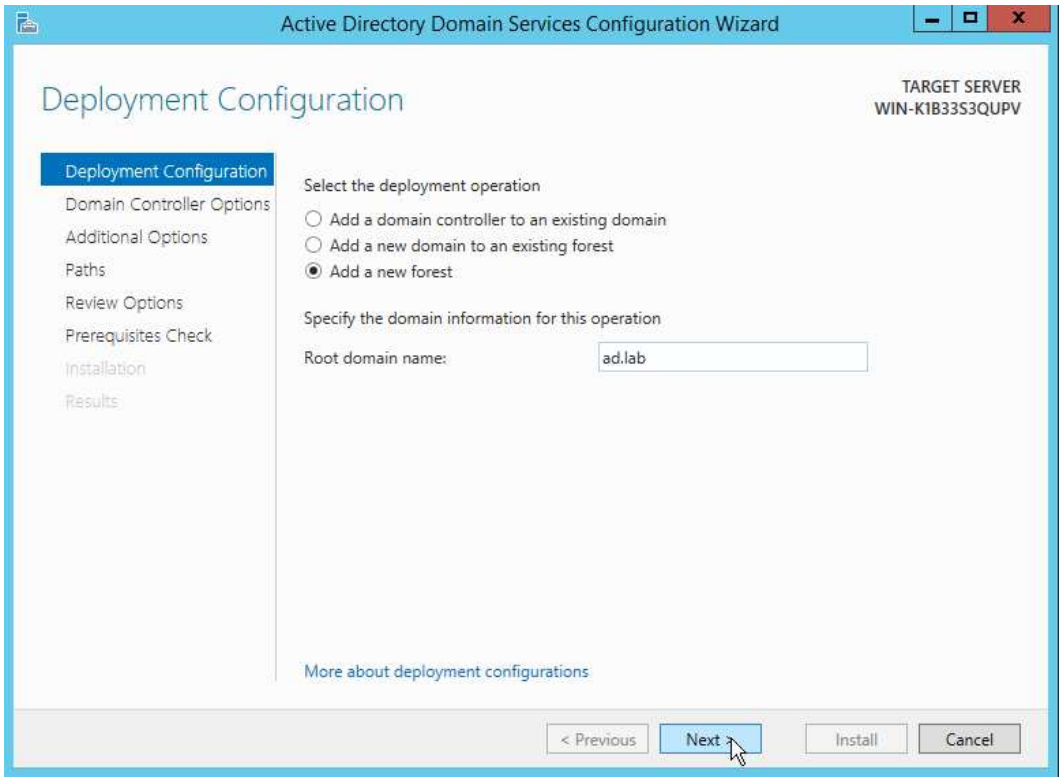
5. Lopuksi käydään läpi lista asennettavista palveluista ja työkaluista sekä asennetaan Active Directory Domain Services.



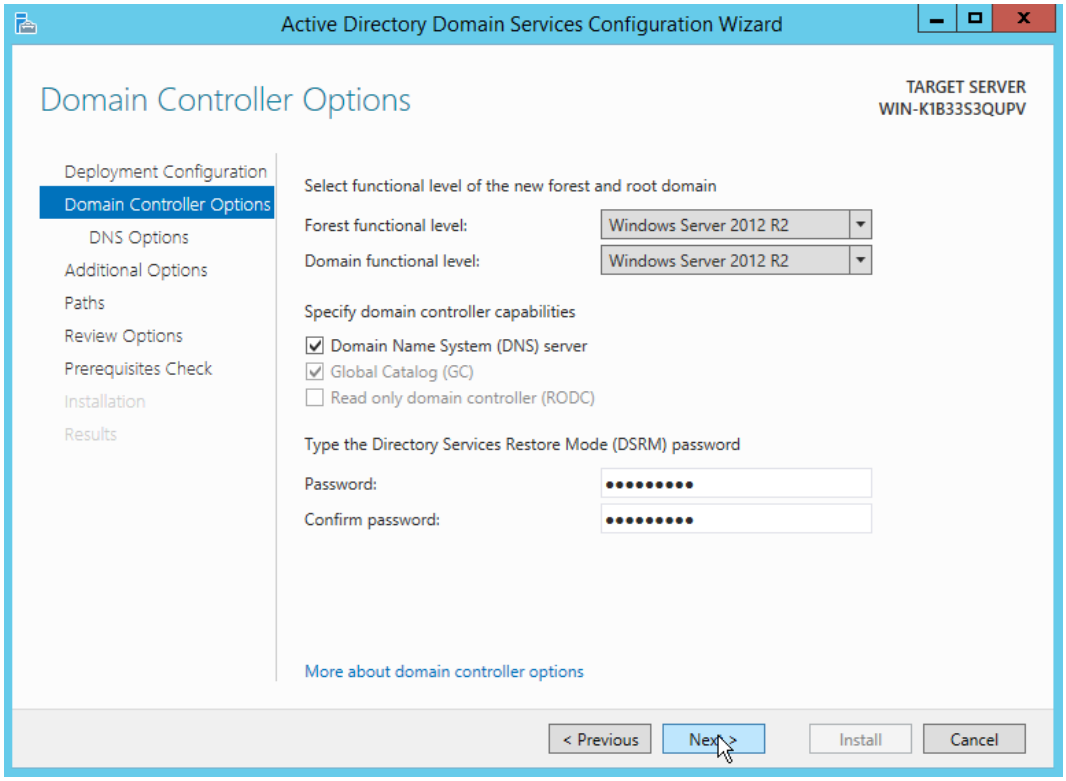
6. Seuraavaksi siirrytään palvelintenhallintaan ja tehdään tarvittavat asennuksen jälkeiset määritykset Active Directory -palvelimelle.



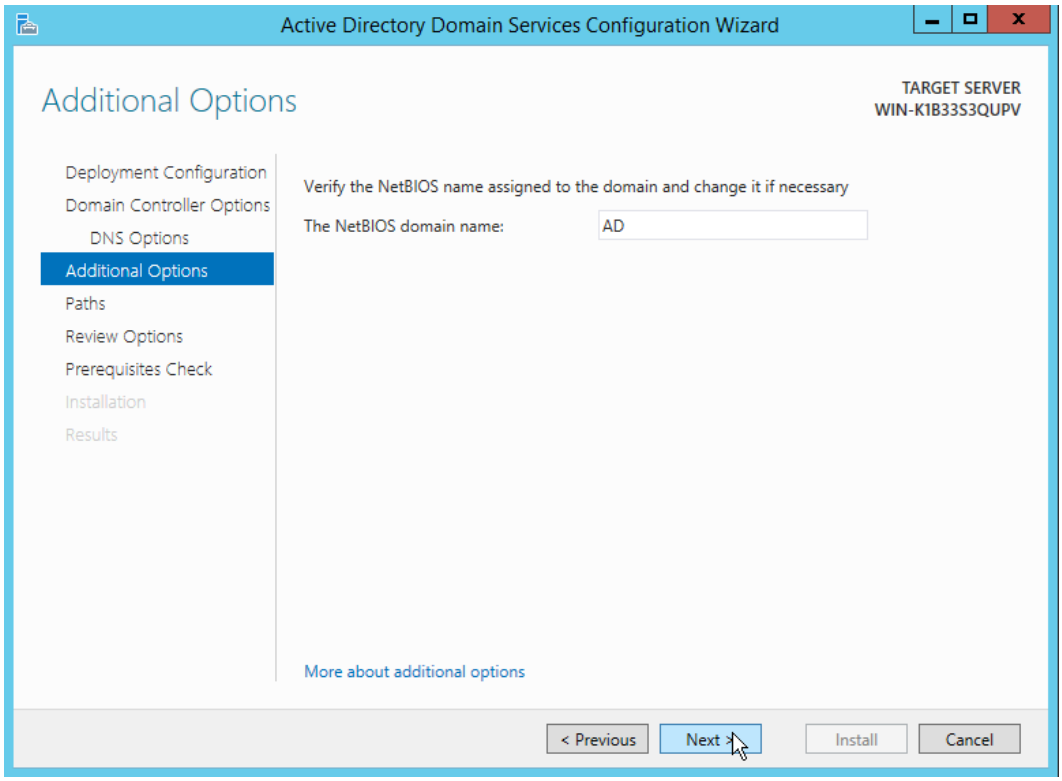
7. Luodaan pääinstanssi Active Directory palvelimelle ja määritetään sille nimi.



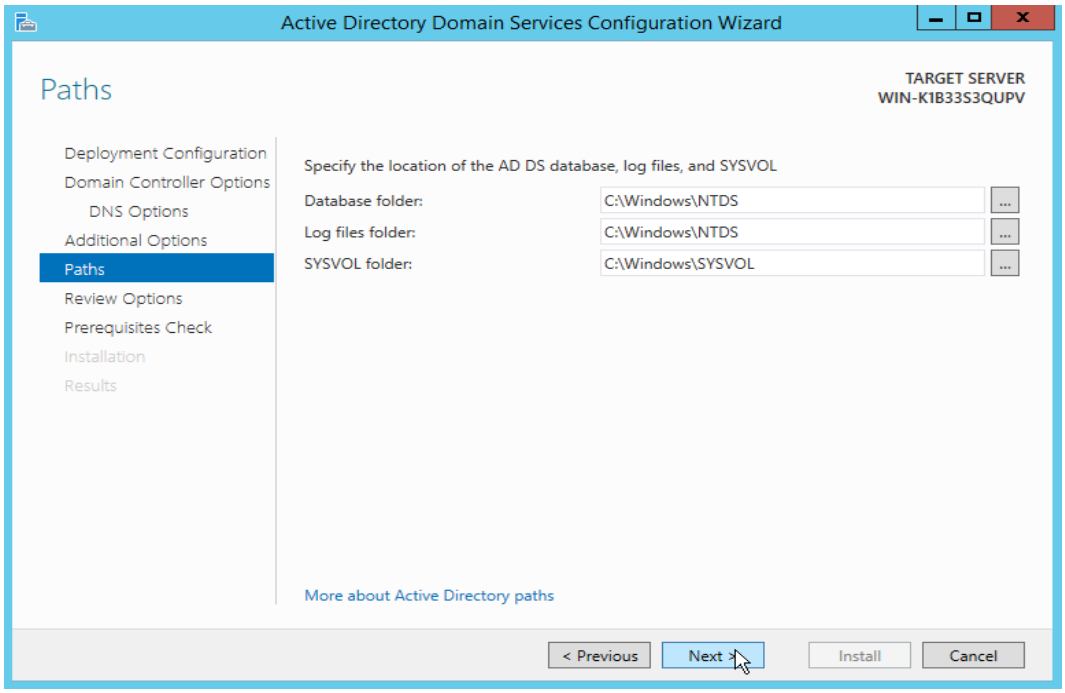
8. Määritetään seuraavaksi, millä tasolla instanssi ja domainit toimivat sekä määritetään DSRM-salasana mahdollista palautustilaa varten.



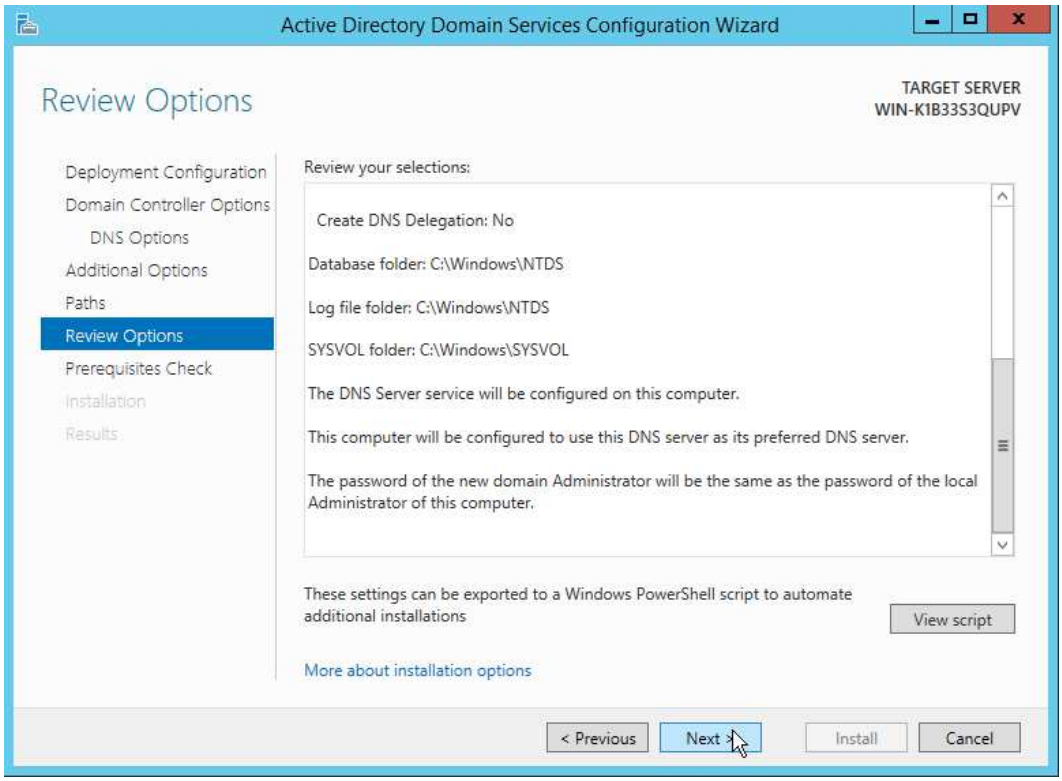
9. Määritetään NetBIOS domain nimi.



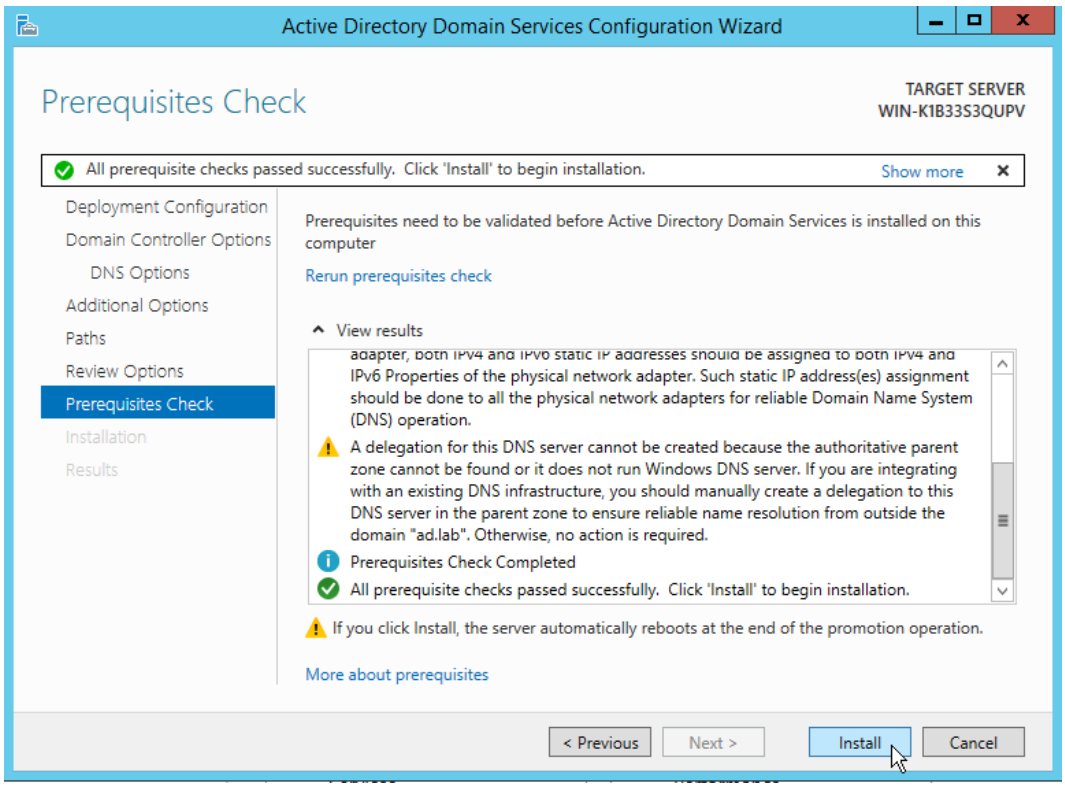
10. Määritetään tiedostopolut tietokannalle, lokitiedostoille ja domainin julkisille tiedostoille (SYSVOL).



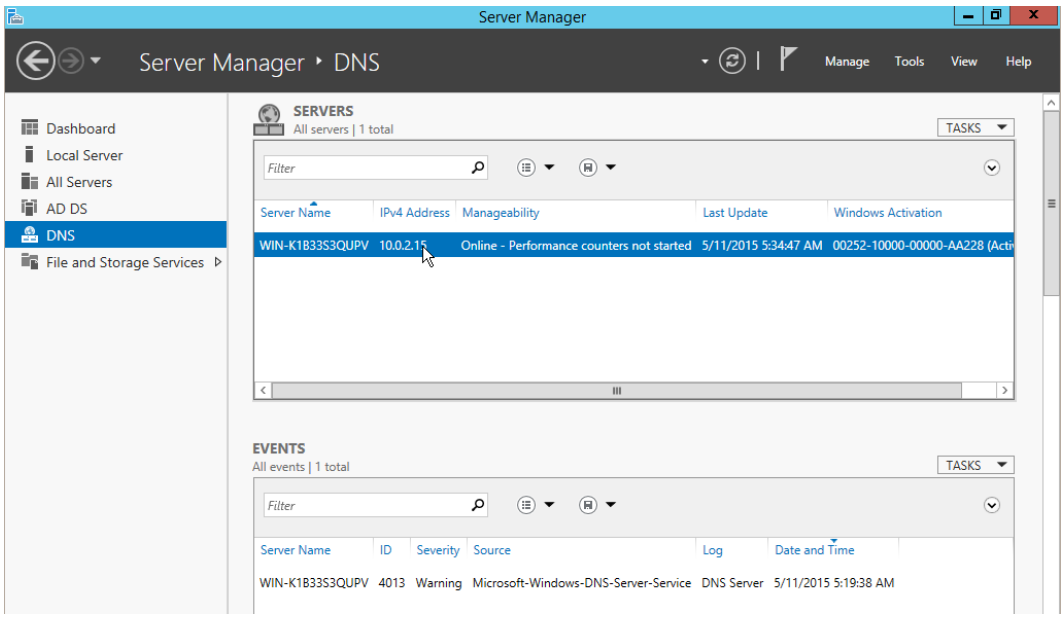
11. Tarkastellaan vielä tehtyjä määrityksiä.



12. Tarkastellaan vielä lopuksi, että kaikki vaatimukset täytetään ennen asennusta.

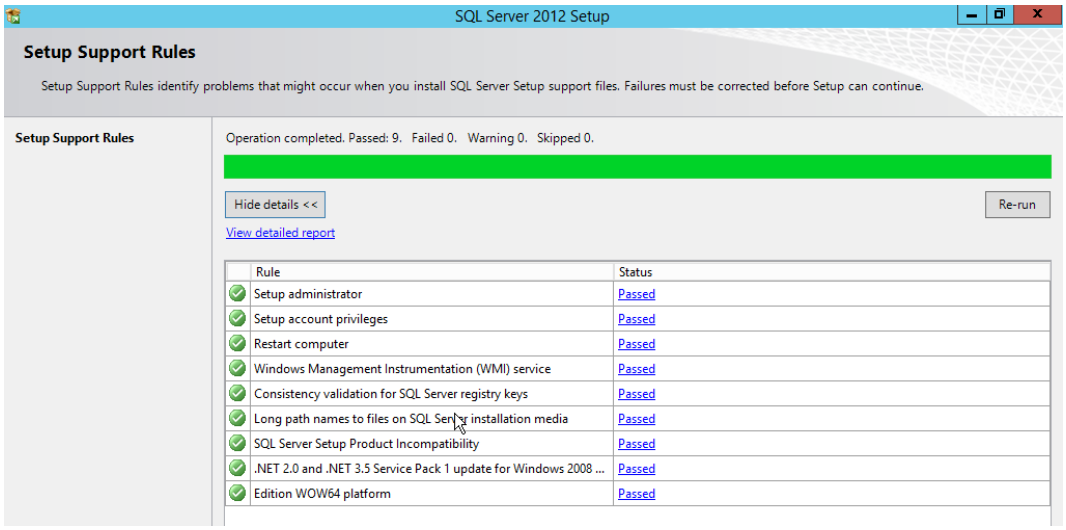


13. Active Directory -palvelimen palvelinhallinnasta voidaan vielä tarkastella, että asennettavat roolit löytyvät ja ovat toiminnassa.



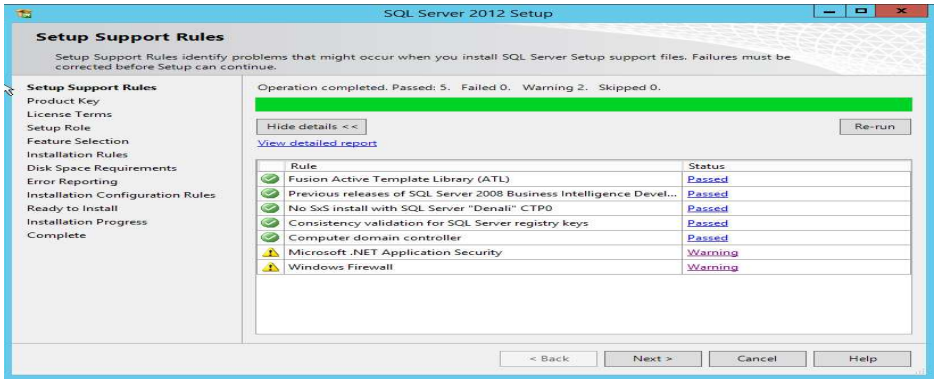
Liite 3. Microsoft SQL Server 2012 -palvelimen asennus

1. Microsoft SQL Server 2012 SQL asennetaan samalle palvelimelle kuin SCOM 2012 R2.

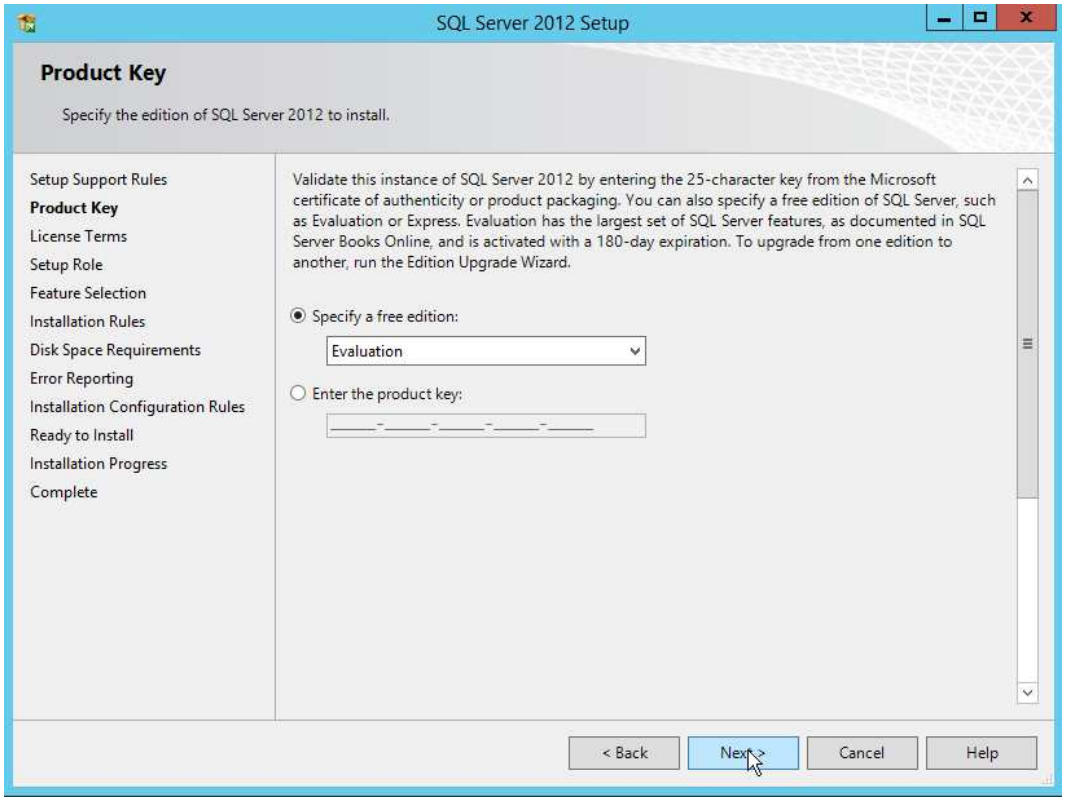


2. Seuraavaksi valitaan asennettavaksi uusi SQL-palvelin kohdasta New SQL Server Stand-alone installation.

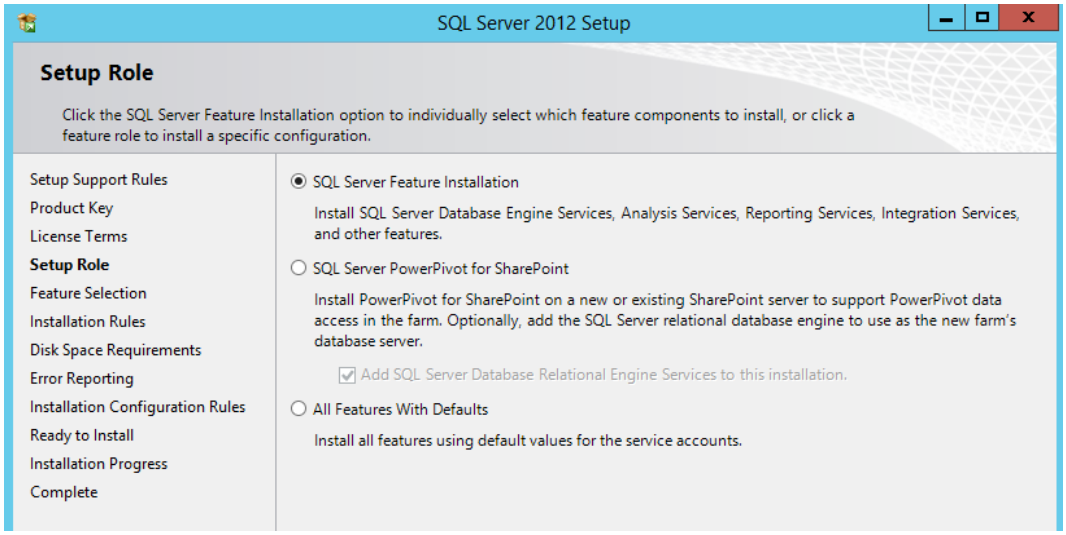
3. Hyväksytään Microsoftin lisenssiehdot ja jatketaan asennusta.



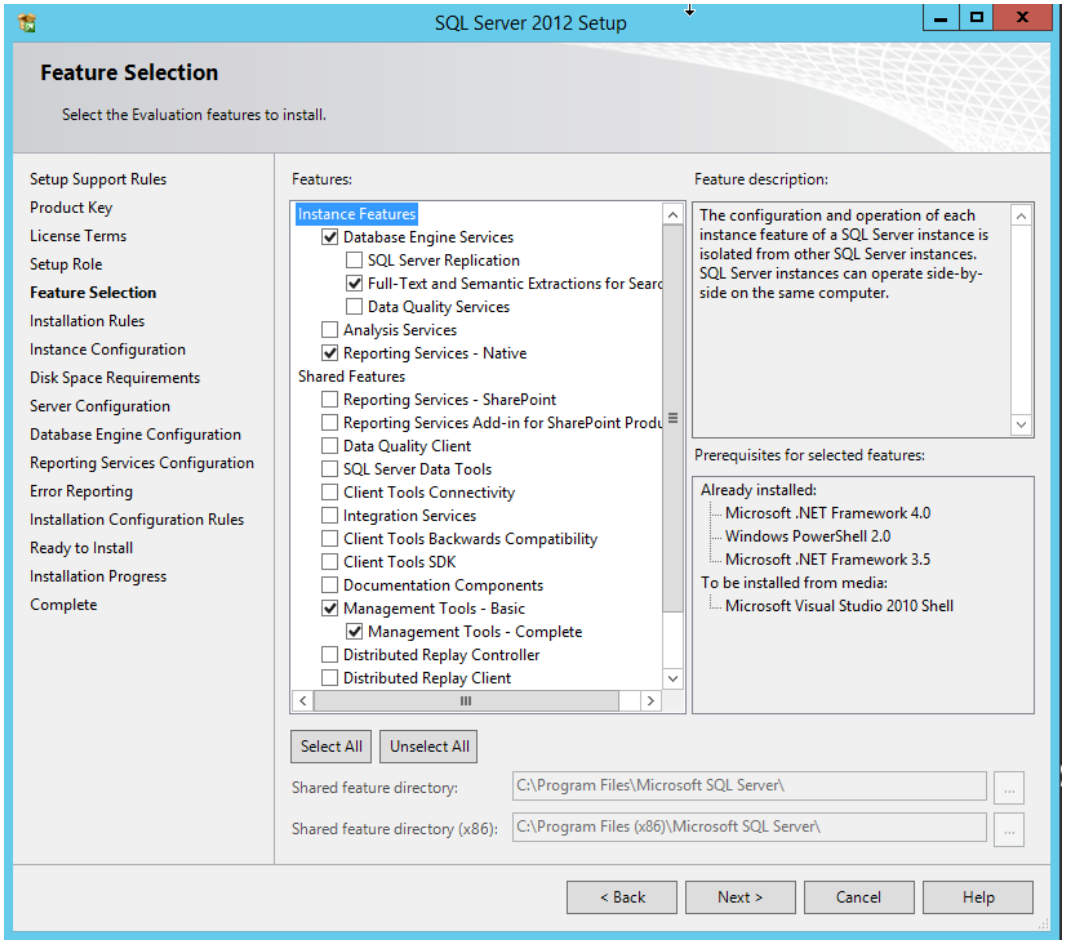
4. Asennusta voidaan jatkaa ja valitaan käytettäväksi ilmainen kokeiluversio.



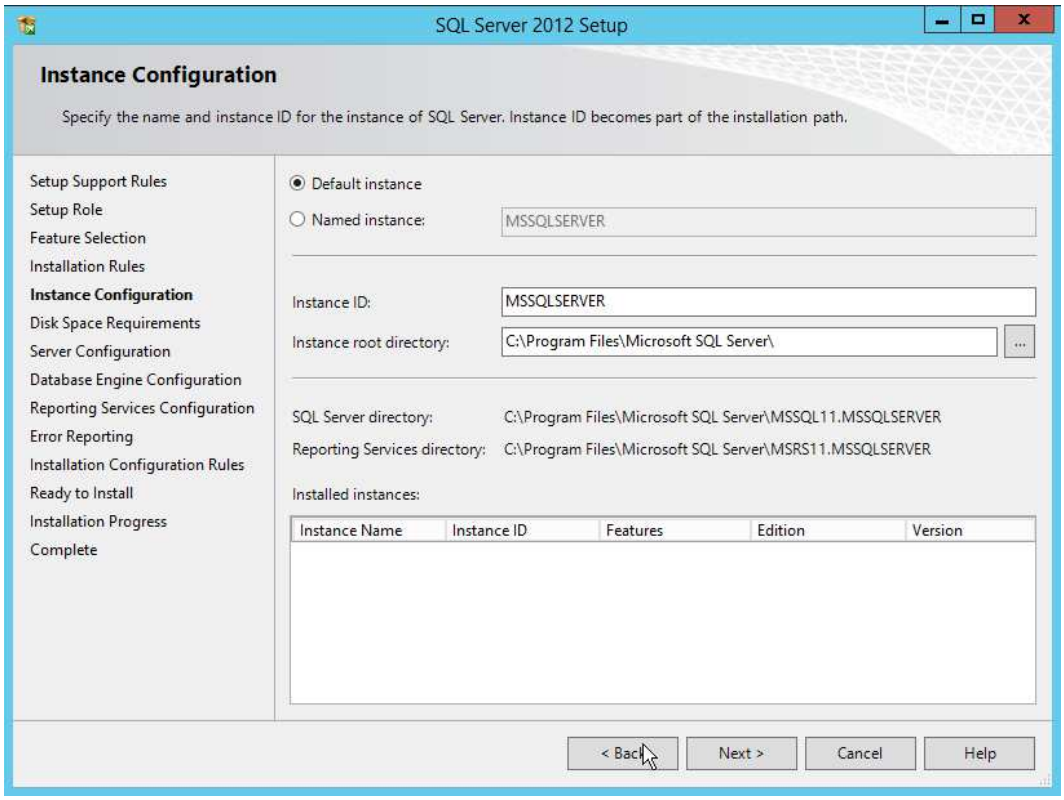
5. Valitaan asennettavaksi SQL Server Feature Installation.



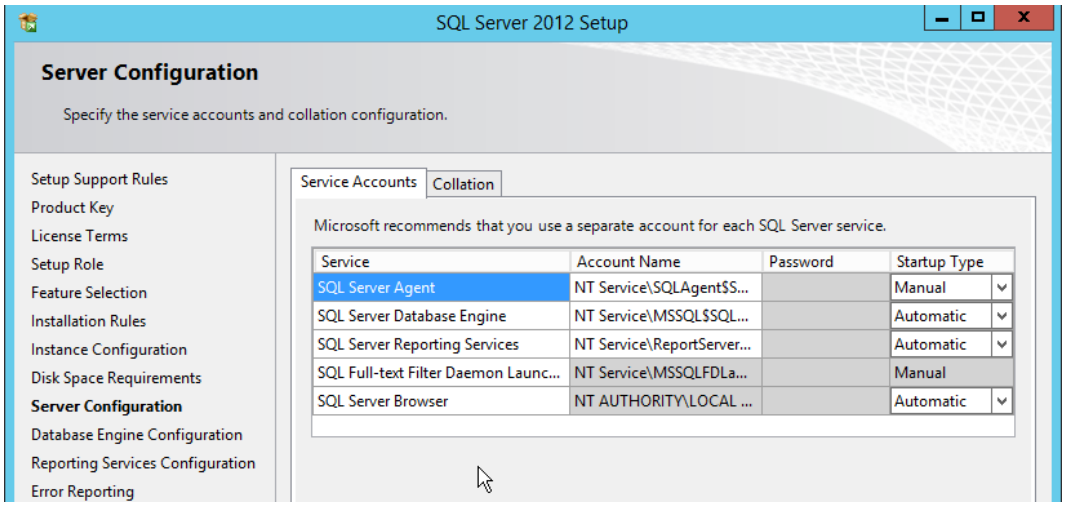
6. Asennetaan toiminnot testiympäristöä varten. Tarvittaessa toimintoja voidaan asentaa lisää.



7. Käytetään SQL-palvelimella vakioitua instanssia MSSQLSERVER. Jos vakioitua SQL-instanssia ei haluta käyttää, luodaan erillinen kohdasta named instance. Nimettyä instanssia varten joudutaan sallimaan pääsy erikseen palvelimelle. Käynnistetään SQL Server Configuration Manager, josta määritellään SQL Server Network Configuration alta TCP/IP asetuksista kohdasta IPALL, TCP-portti 1433 käytettäväksi.

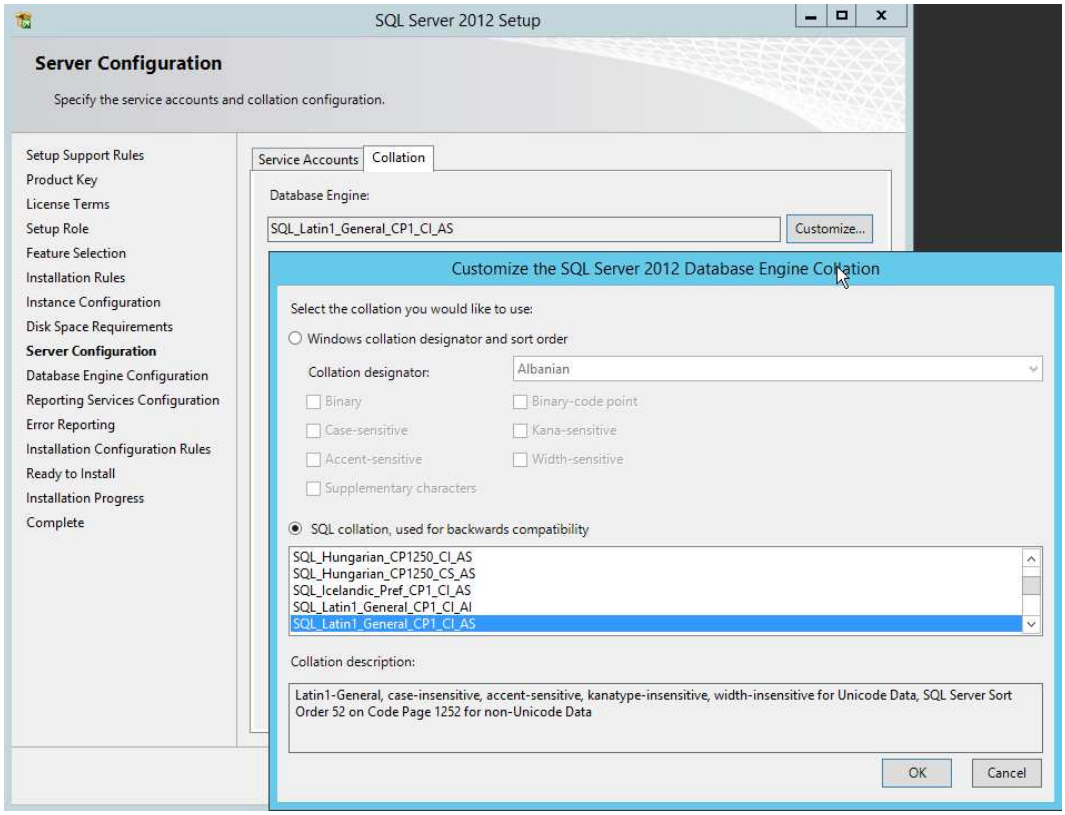


8.Jatketaan palvelimen asennusta ja määritetään Server Configuration kohdasta Service Accounts -välilehdeltä SQL-palvelimen palveluiden käyttämät tunnukset.

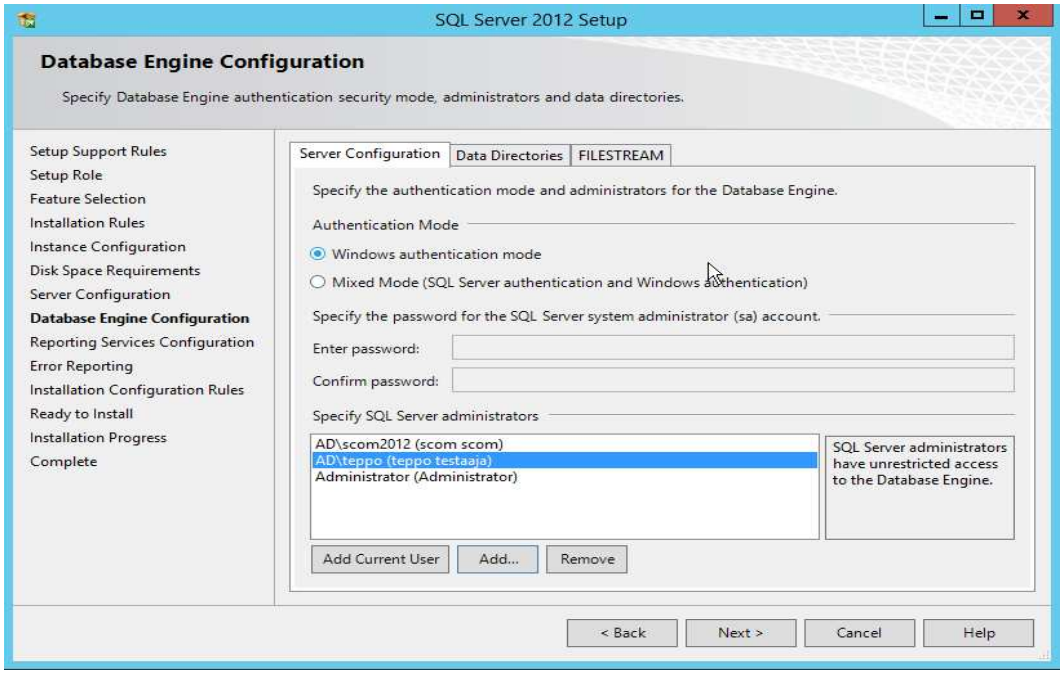


9. Collation välilehdeltä valitaan palvelimen käyttämät säännöstöt. Valittaessa säännöstä on huomioitavaa, että on suositeltavaa valita ”SQL_Latin1_General_CP1_CI_AS”Uusi versio SCOM 2012 R2 tukee jo

useampaa säännöstöä, mutta vanhemmat versiot SCOM työkalusta eivät toimi oikein.

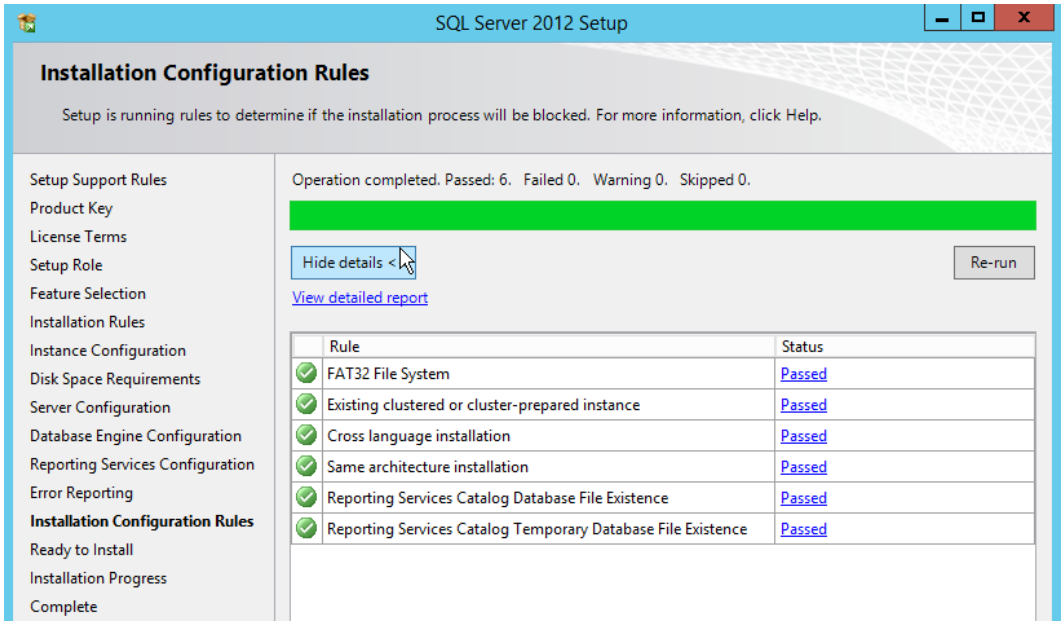


10. Database Engine Configuration kohdasta määritellään käytettäväksi Windowsin oma tunnistautuminen ja määritellään myös SQL-palvelimen ylläpitäjät käyttäen esimerkiksi domain- ja paikallisia tunnuksia.

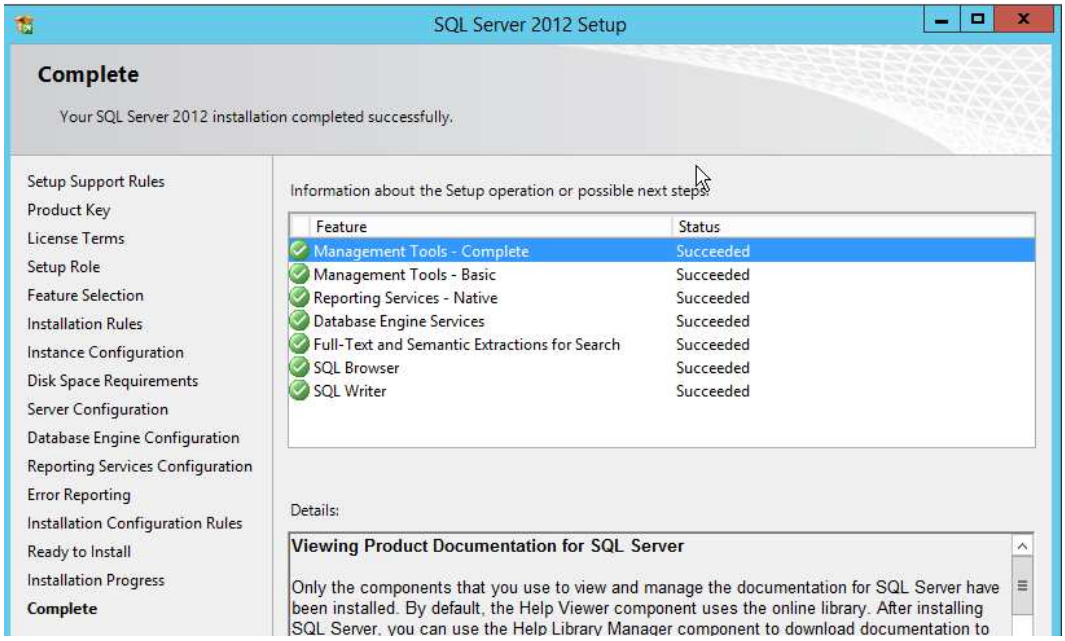


11. Seuraavaksi asennetaan Reporting Services raportointia varten, jotta SCOM työkalulla voidaan muodostaa historiallisia raportteja.

12. Valitaan vielä lopuksi ettei raportointia virheistä lähetetä Microsoftille ja tarkistetaan asennuksen säännöt vielä läpi onnistuneesti.



13. Kun kaikki kohdat on käyty lävitse onnistuneesti voidaan lopuksi voidaan tehdä palvelimen lopullinen asennus.

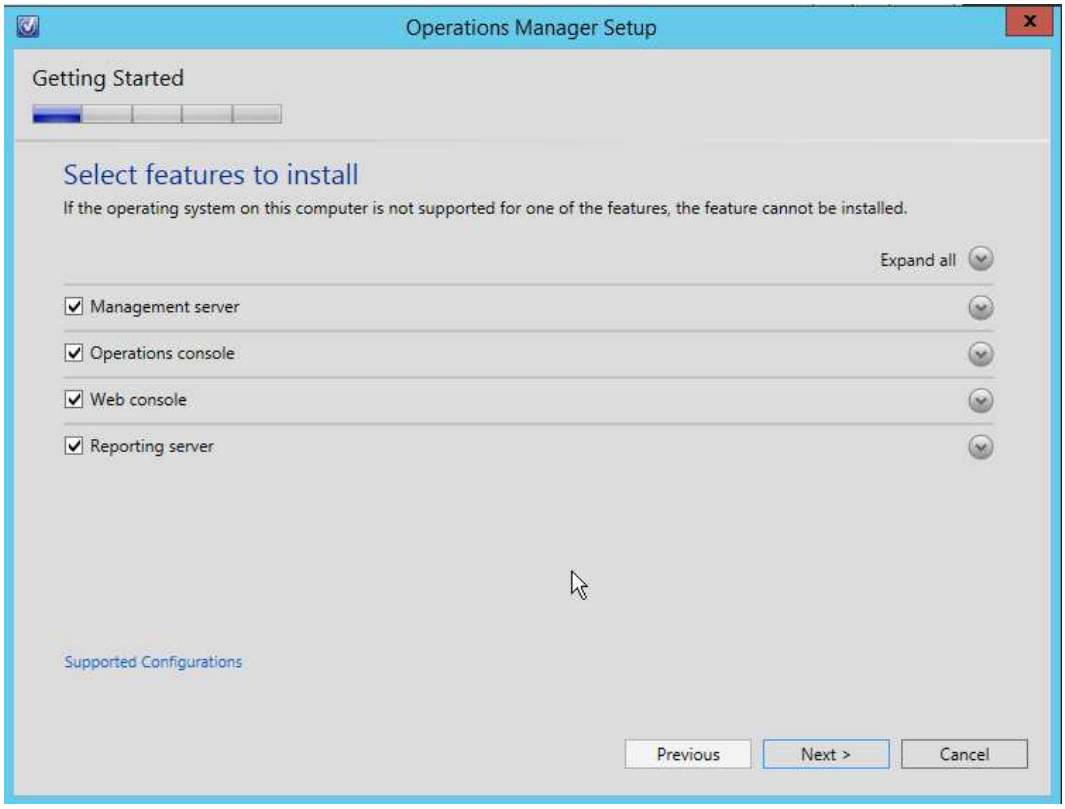


SQL-palvelinta ja tietokantoja voidaan hallita SQL Server Management Studio- ja SQL Server Configuration Manager työkaluilla.

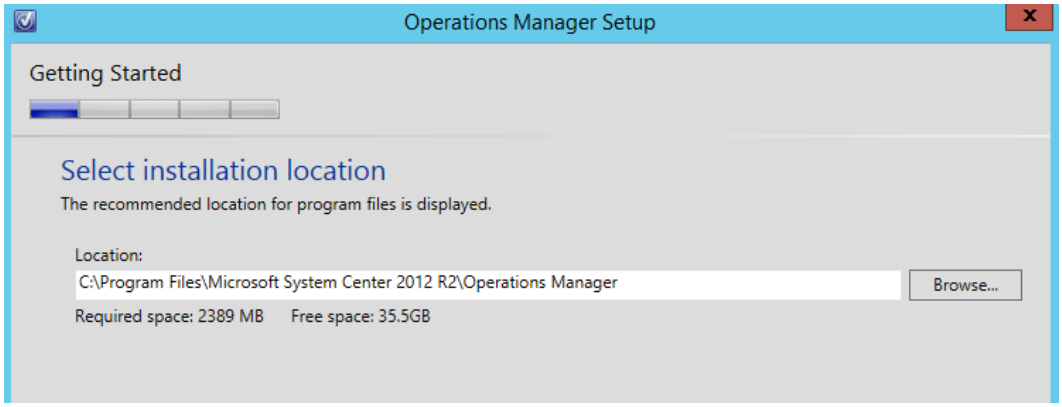
Liite 4. SCOM 2012 R2 -palvelimen asennus

1. Kun kaikki vaadittavat roolit ja toiminnot, Active Directory Domain Services, Microsoft SQL Server 2012 on asennettuna voidaan aloittaa SCOM 2012 R2 asennus.

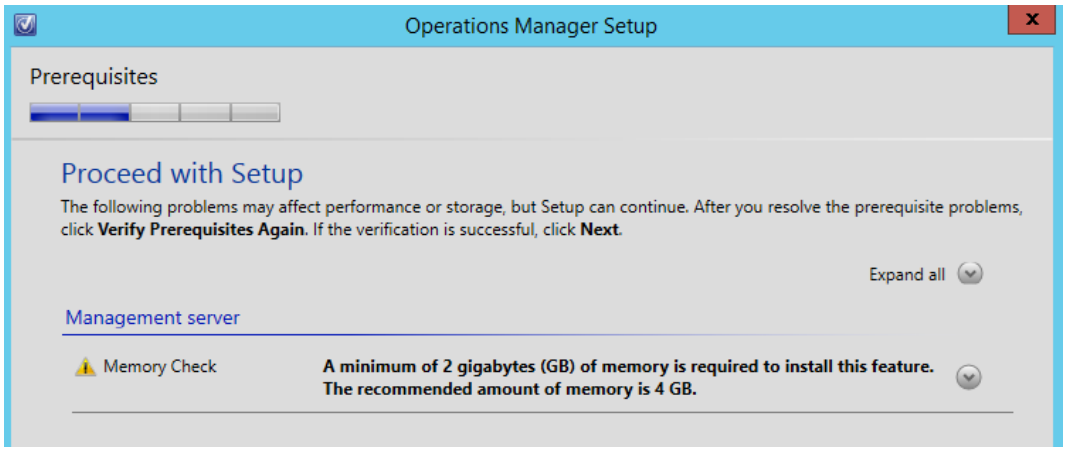
2. Asennukseen valitaan kaikki toiminnot: management server, operations console, web console ja reporting services.



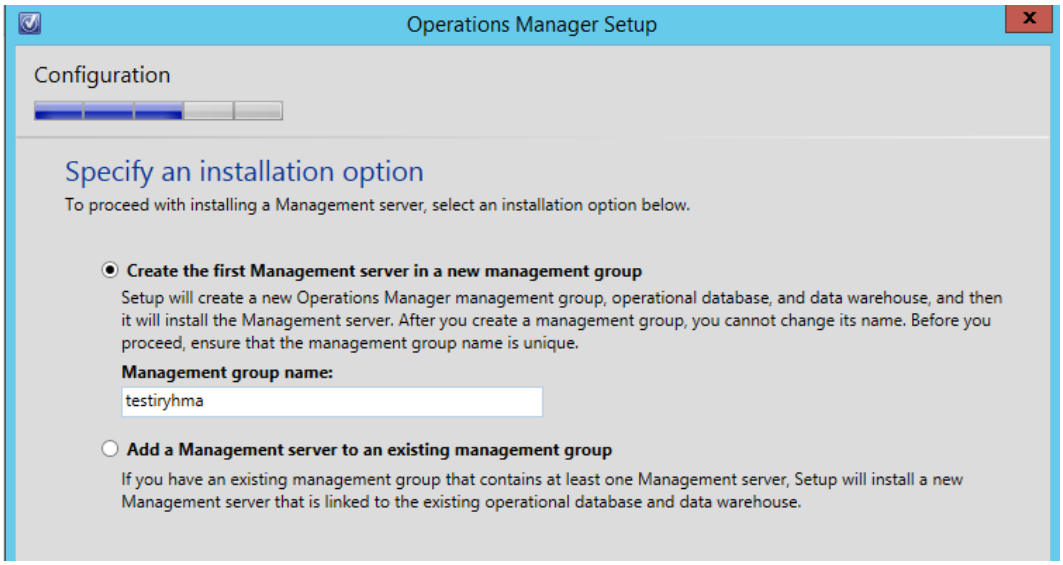
3. Määritetään SCOM 2012 R2 asennukselle polku paikalliselle virtuaalikoneen levylle.



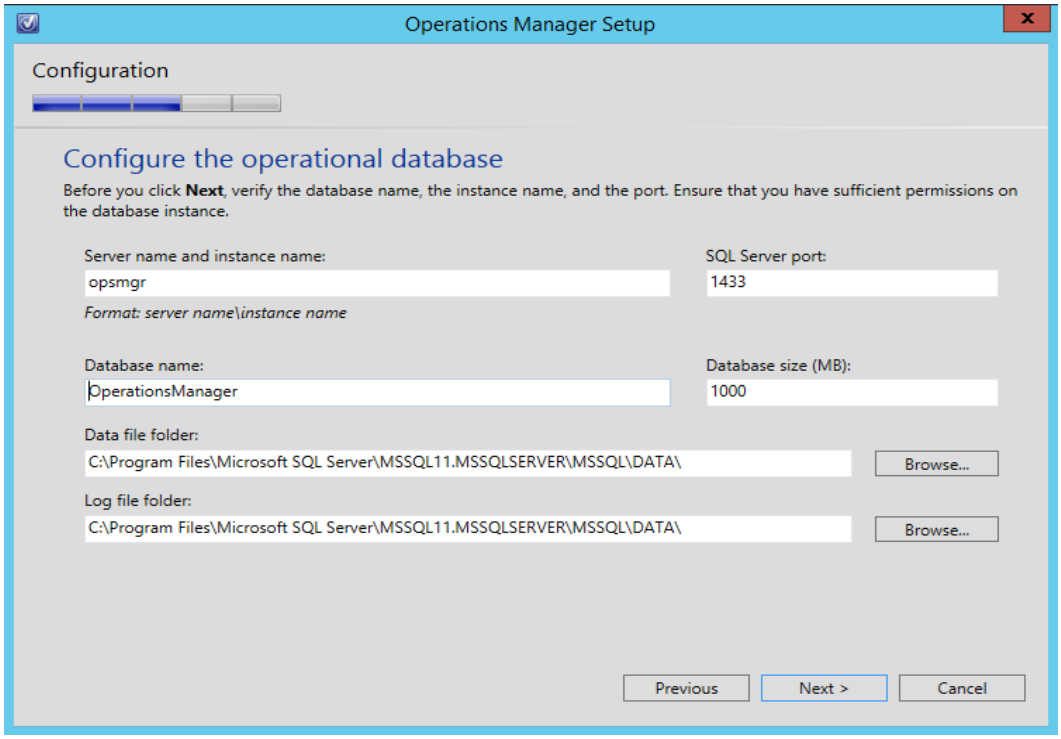
4. Asennusohjelma käy läpi tarvittavat hallintapalvelimen vaatimukset ja suositukset.



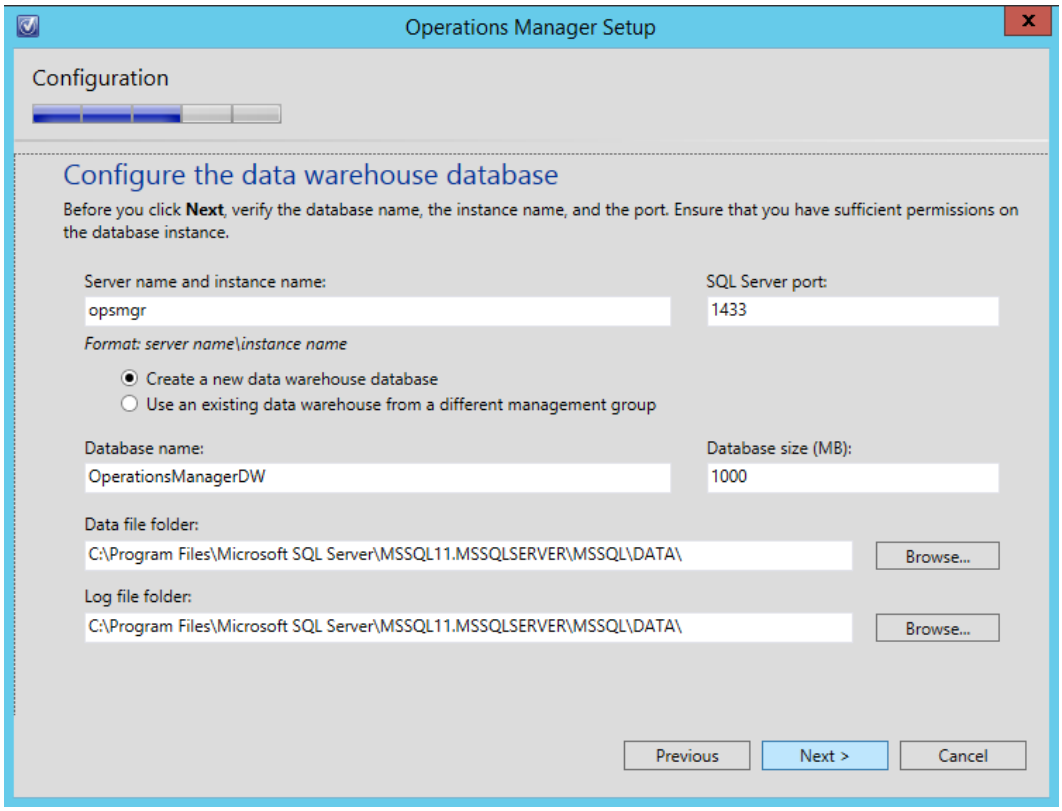
5. Seuraavaksi määritetään uuden hallintapalvelimen käyttämä hallintaryhmän nimi. Jälkeenpäin on mahdollista asentaa muita hallintapalvelimia ja liittää ne jo olemassaolevaan hallintaryhmään, jolloin saavutetaan haluttaessa kuormantasausta ja vikasietoisuutta SCOM 2012 R2 -palvelinten kesken. Hyväksytään hallintaryhmän luonnin jälkeen lisenssiehdot.



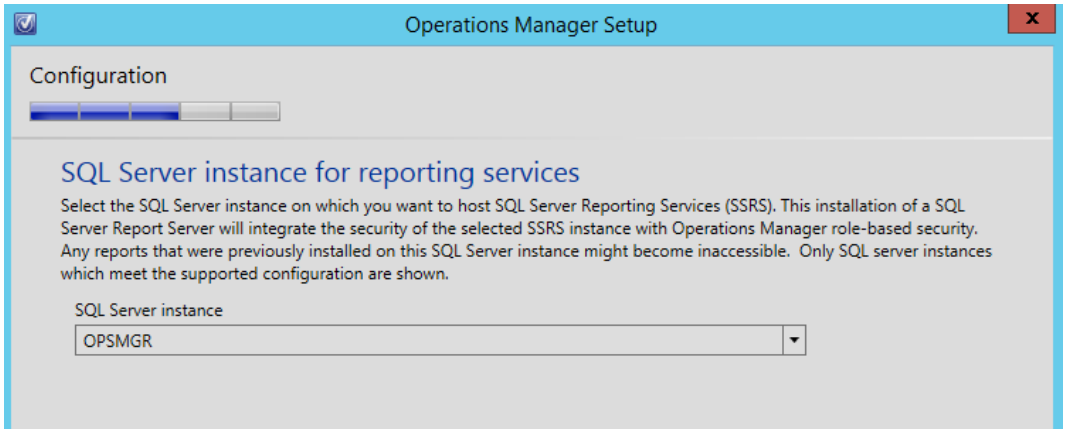
6. Määritellään seuraavaksi operational -tietokanta. Määritellään palvelimen nimi ja käytetään paikallisen SQL-palvelimen oletusporttia. Käytetään myös tietokantaan oletusnimeä ja kokoa.



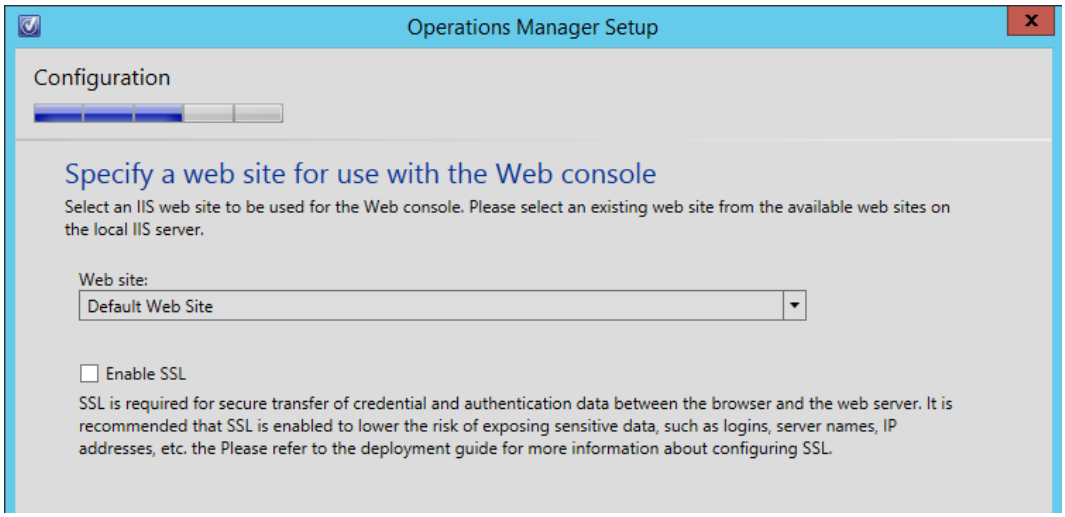
7. Määritellään myös data warehouse -tietokanta historiallista raportointia ja analysointia varten samat asetukset kuin operational-tietokannassa ja käytetään oletusnimeä tietokannassa



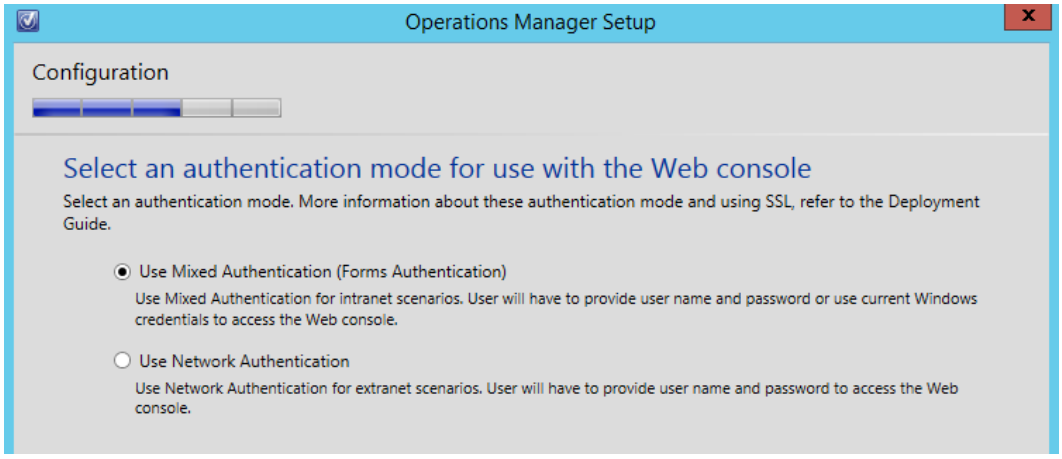
8. Valitaan SQL Server instanssi raportointi palveluja varten.



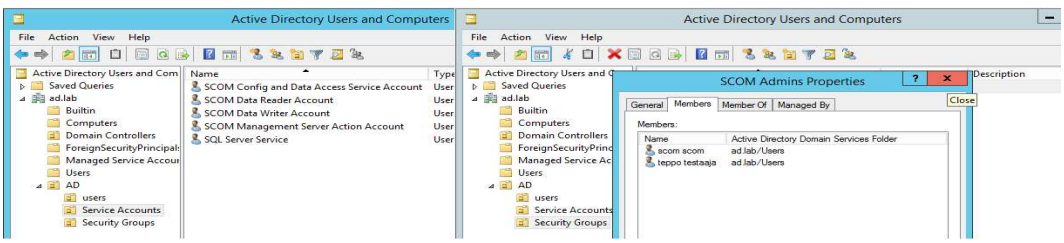
9. Instanssin jälkeen määritellään, mitä sivustoa Web Console käyttää. Tässä tapauksessa testiympäristössä on vain yksi sivusto käytössä niin voidaan käyttää oletussivustoa. Testiympäristössä HTTP -istuntojen salausta (SSL) ei oteta käyttöön, mutta tuotannollisessa tai avoimessa ympäristössä salaus on ehdoton. Salaus voidaan tarvittaessa määritellä IIS-palvelimella, jolle luodaan sertifikaatit ja asennetaan ne.



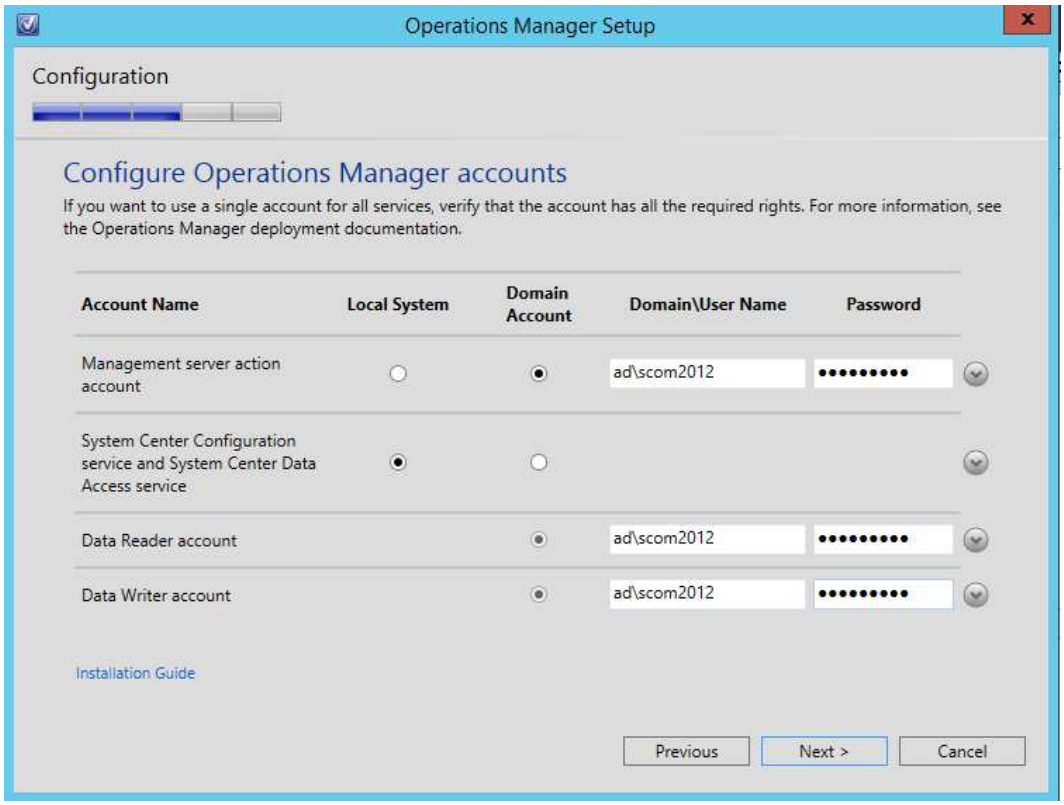
10. Web consolea varten otetaan käyttöön ”Mixed Authentication”.



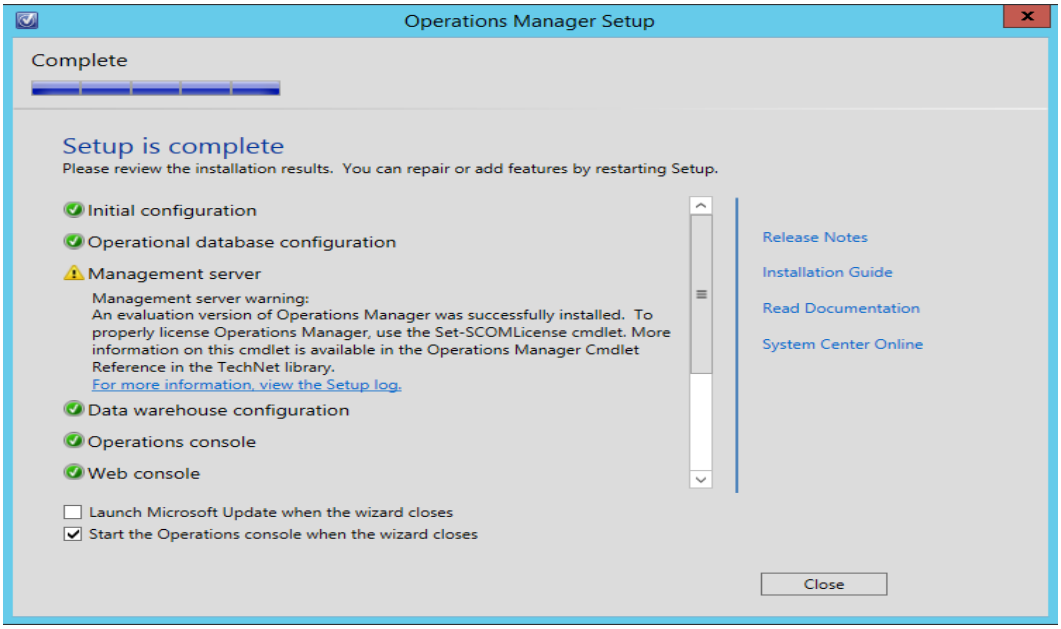
11. Lopuksi määritellään käytettävät SCOM-tunnukset. Suljetussa testiympäristössä käytetään yksinkertaistamiseksi samaa domain admin -tunnusta. Tuotannollisessa ympäristössä tietoturvallisesta näkökulmasta tulisi jokaiselle viidelle SCOM -toiminnolle luoda oma tunnus: Data Writer, Data Reader, Data Access, Management Server Actions ja SQL-palvelutunnus. Jokaisen tunnuksen oikeudet tulisi rajoittaa vastaamaan vain käytettyä toimintoa



.

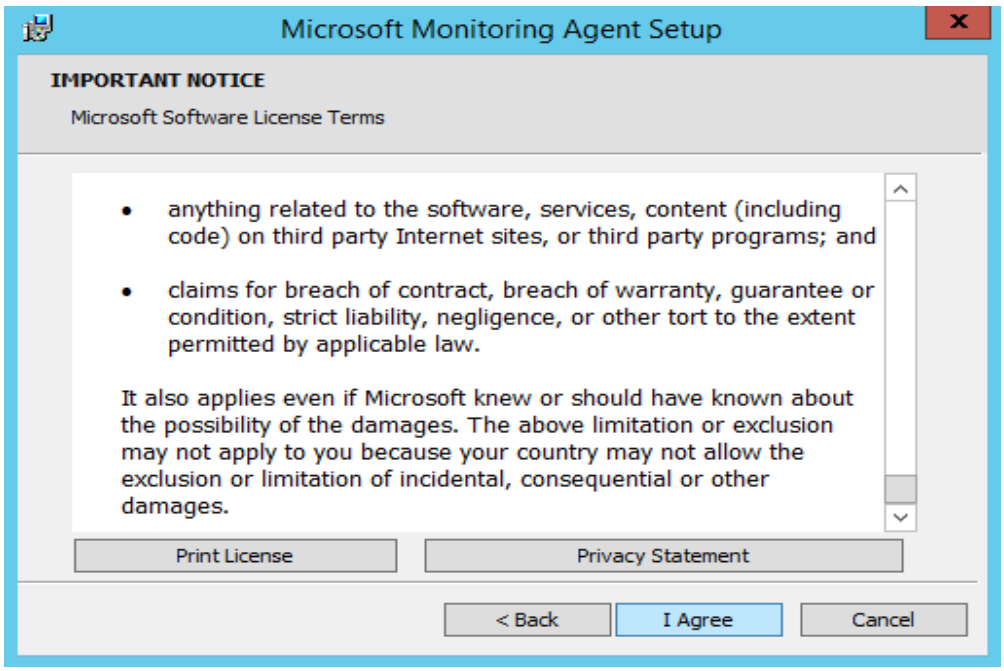


12. Tunnusten määritysten jälkeen kielletään vielä Microsoftin automaattisten päivitysten käyttö ja hoidetaan ne tarvittaessa manuaalisesti. Asennuksen lopuksi voidaan tarkastella asennuksen tuloksia ja tarvittaessa osasia voidaan myös jälkeenpäin asentaa lisää käynnistämällä asennusohjelma uudelleen.

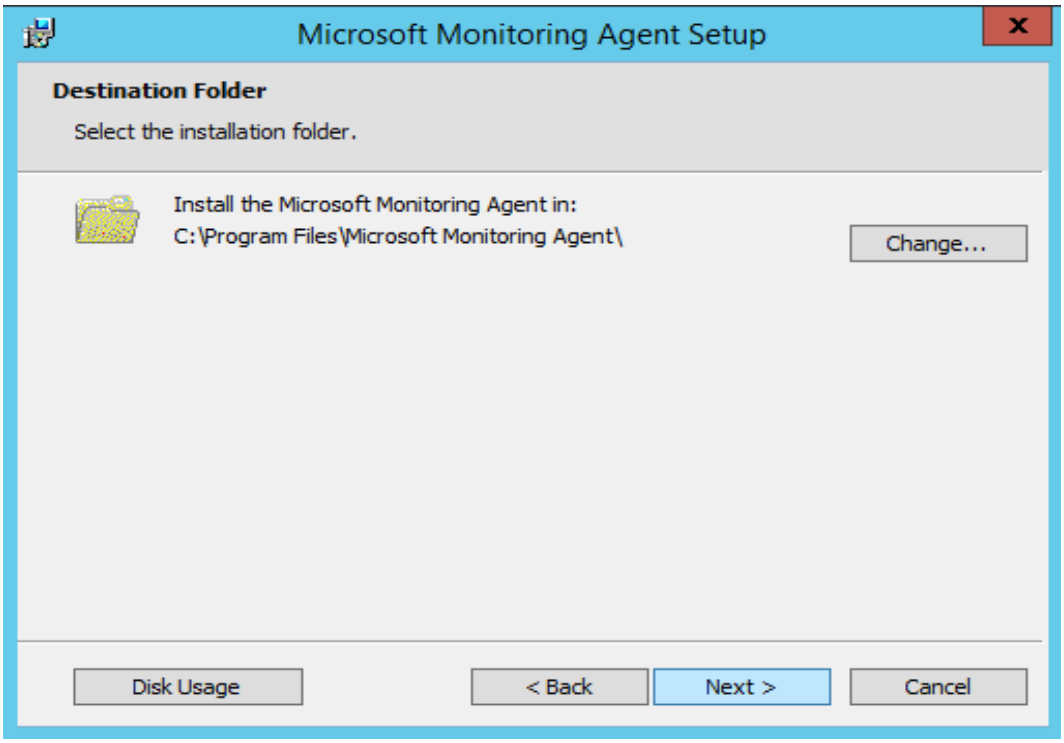


Liite 5. SCOM 2012 R2: valvonta-agenttien asennus ja määrittely

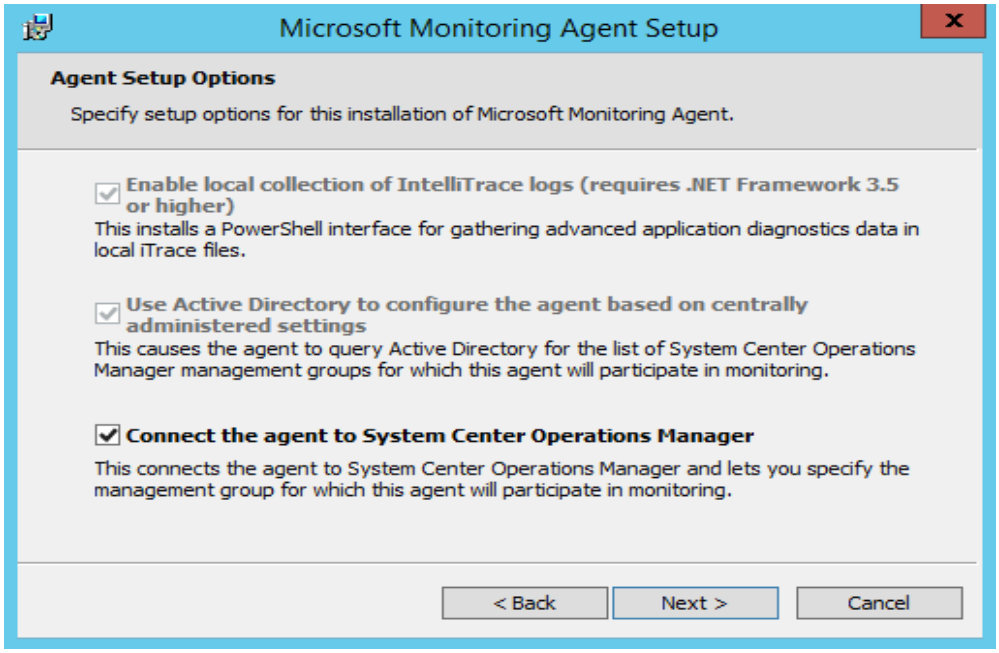
1. Käynnistetään Microsoft Monitoring Agent –asennusohjelma SCOM 2012 R2 medialta.



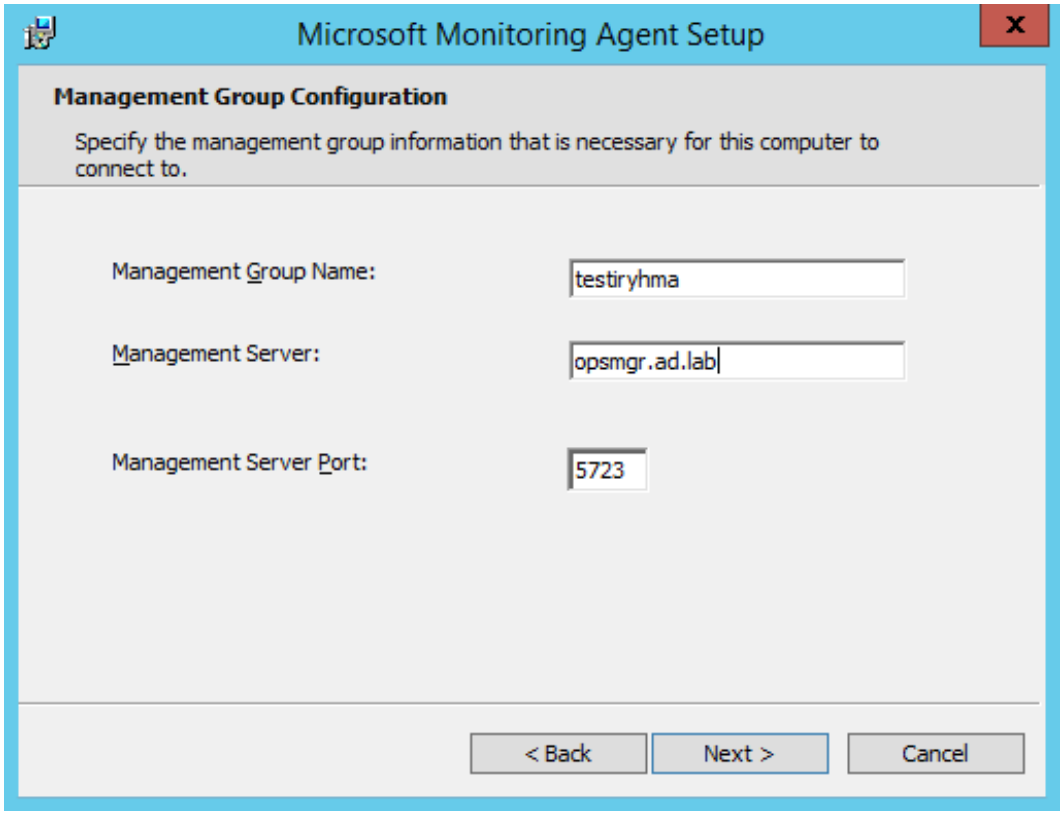
2. Asennetaan Microsoft Monitoring Agent paikalliselle virtuaalikoneen levylle.



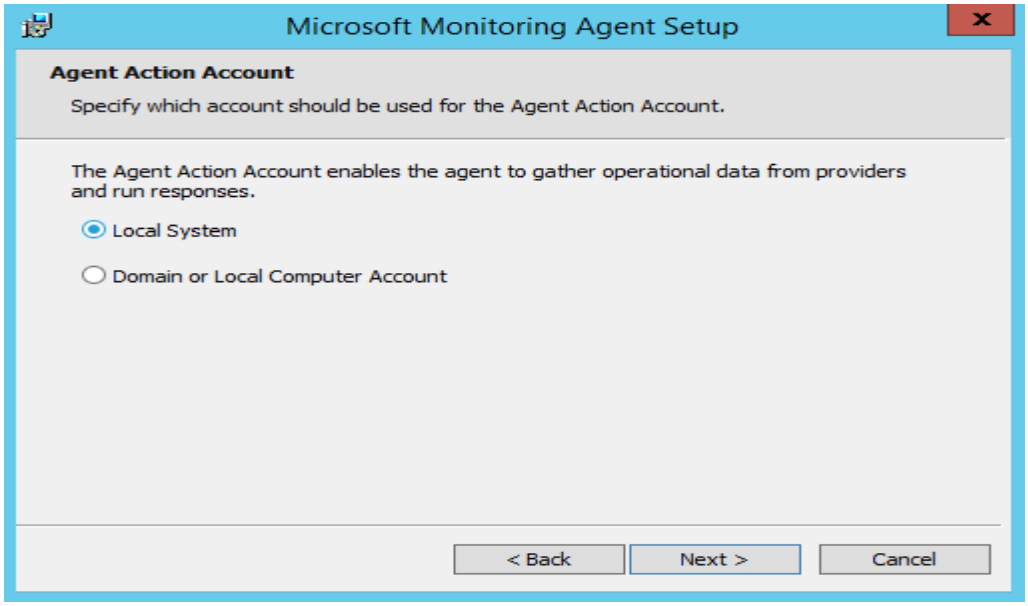
3. Yhdistetään seuraavaksi Microsoft Monitoring Agent SCOM 2012 R2 palvelimelle.



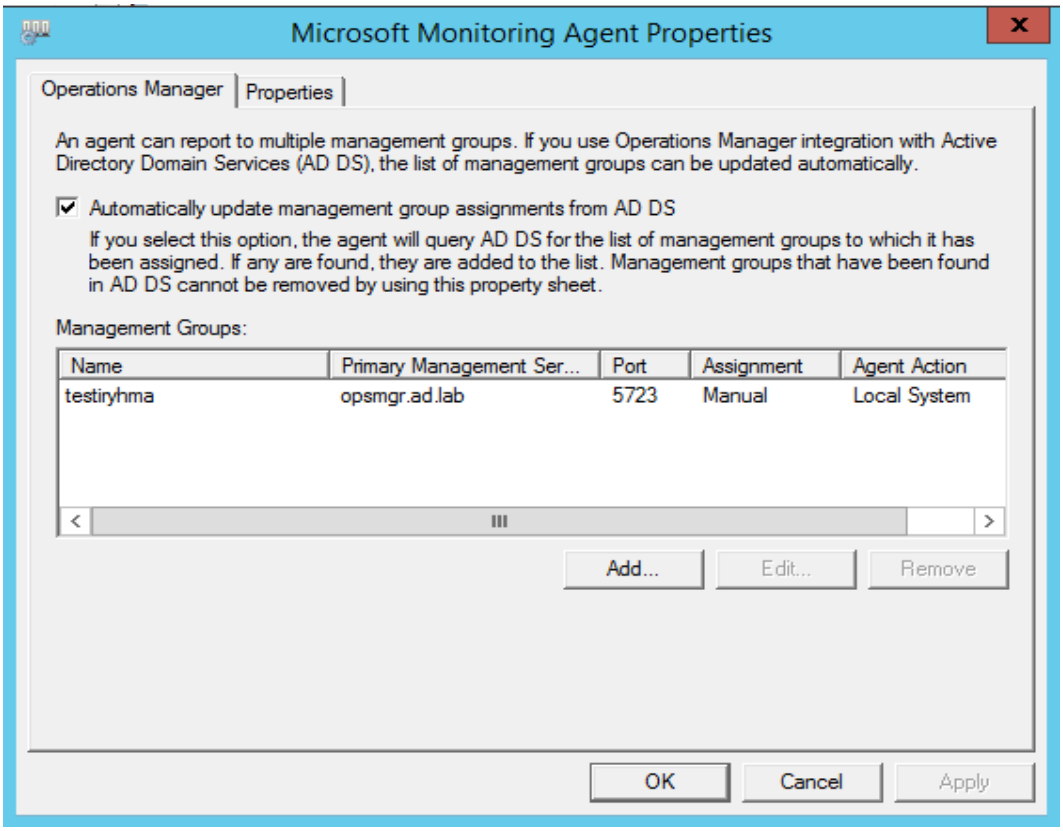
4. Agentille määritetään hallintaryhmän nimi, hallintapalvelimen nimi sekä hallintapalvelimen portti.



5. Seuraavaksi määritetään käyttäjätunnus, jota agentti käyttää valvontaan.

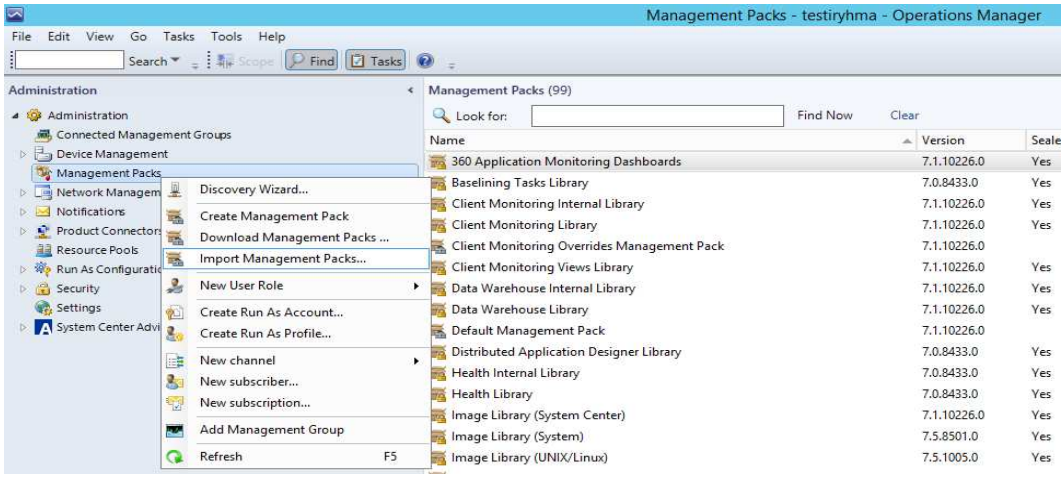


6. Asennetun Agentin asetuksia voidaan tarkastalle Windowsin hallintapaneelista kohdasta Microsoft Monitoring Agent. Muutoksia voidaan tehdä jälkeenpäin tarvittaessa.

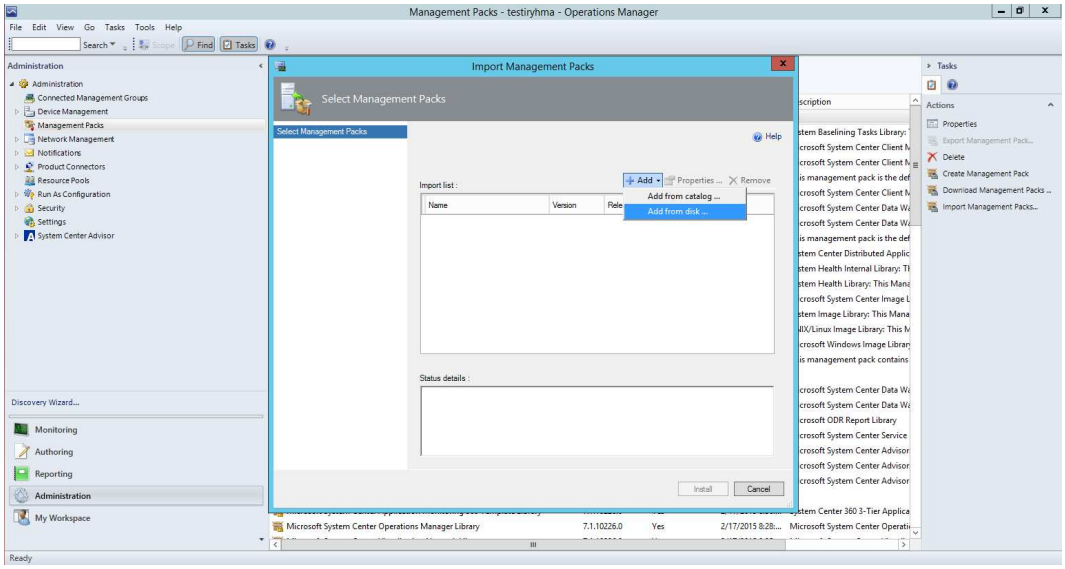


Liite 6. SCOM 2012 R2: hallintapakettien asennus ja kohteen lisäys

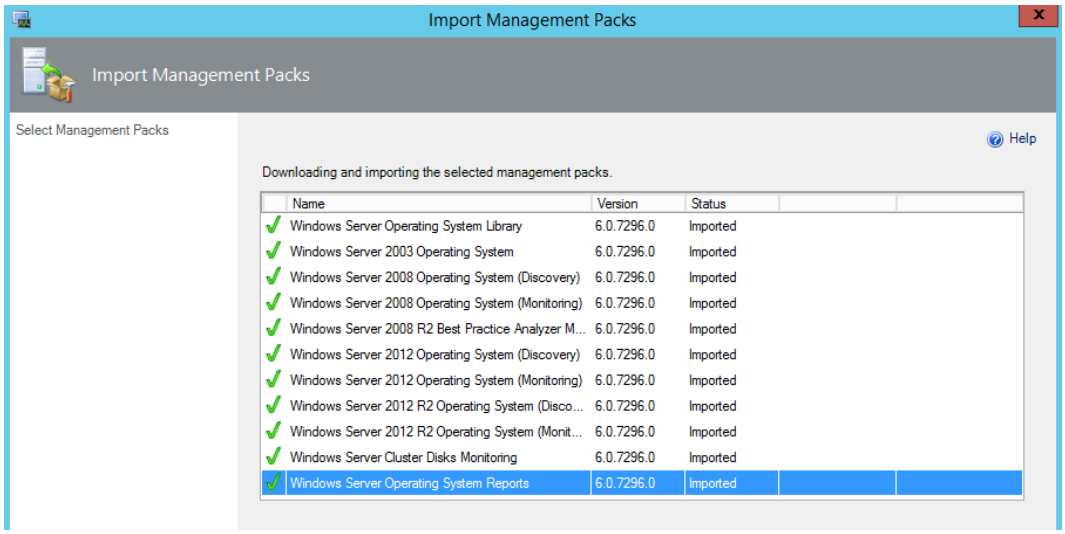
1. Valitaan import management pack.



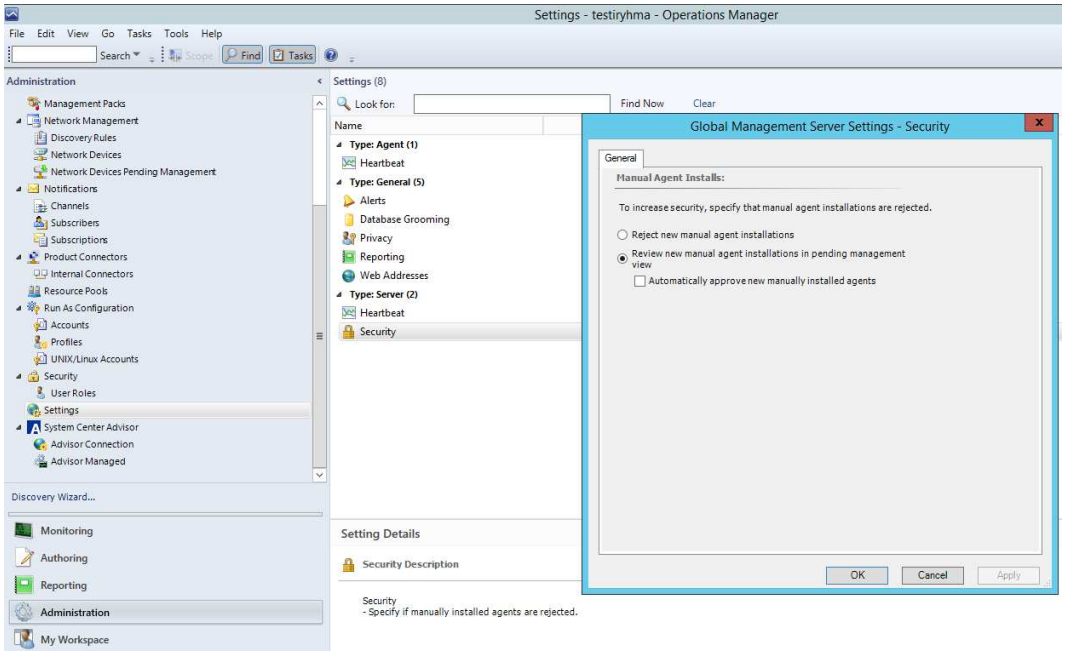
2. Seuraavaksi valitaan haluttu hallintapaketti, joka asennetaan. Valitaan Windows palvelusta valmiiksi ladattu hallintapaketti paikalliselta kovalevyltä. Jos hallintapaketilla on riippuvuisuuksia toisiin hallintapaketteihin on helpointa käyttää katalogia.



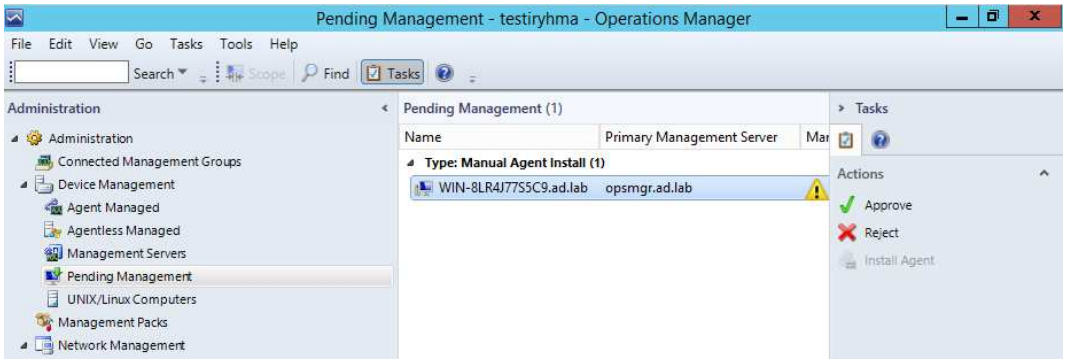
3. Valitut hallintapaketit on nyt asennettuina ja kyseisen hallintapaketin sisältämiä kohteita voidaan nyt havaita ja suorituskykytietoja lukea.



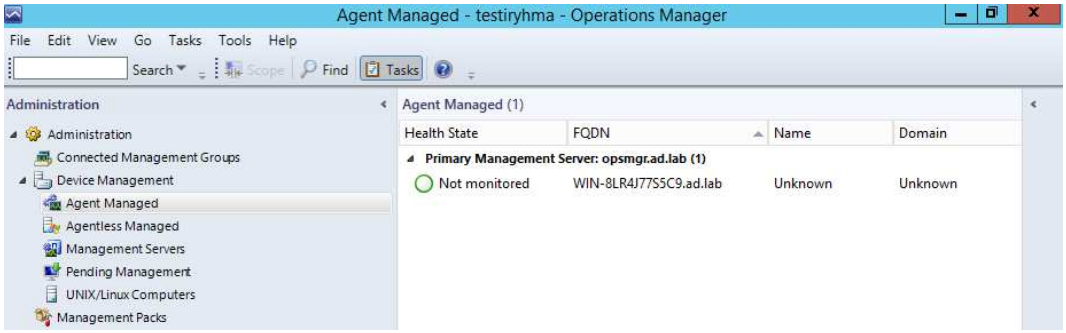
4. Valitaan Administration ja navigaatio ikkunasta settings. Tulosruudusta valitaan settings, josta voidaan asettaa kuinka manuaalisesti asennettujen agenttien kohdalla toimitaan. Valitaan agentit hyväksyttyväksi manuaalisesti.



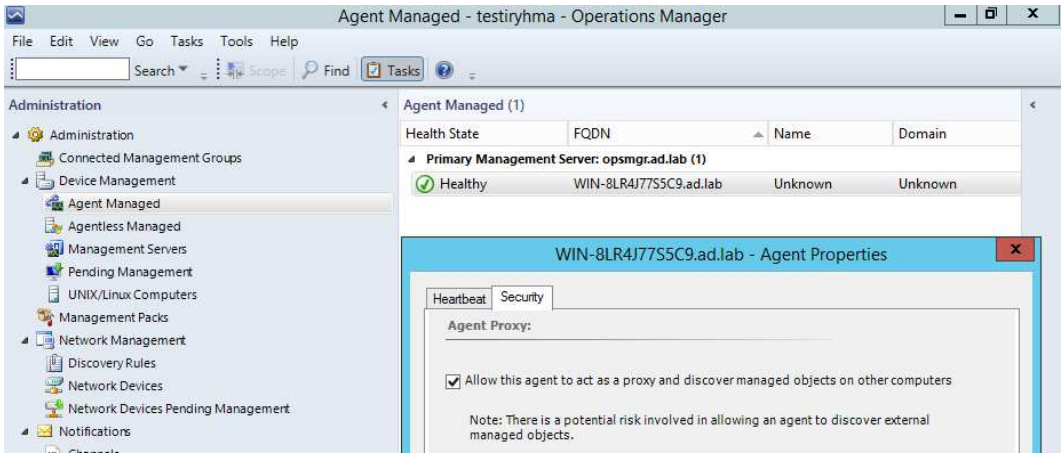
5. Kun hallintapalvelin on havainnut valvottavan kohteen se hyväksyä ja lisätä valvontaa.



6. Valvottavaksi hyväksytty kohde siirtyy hallittaviin kohteisiin.

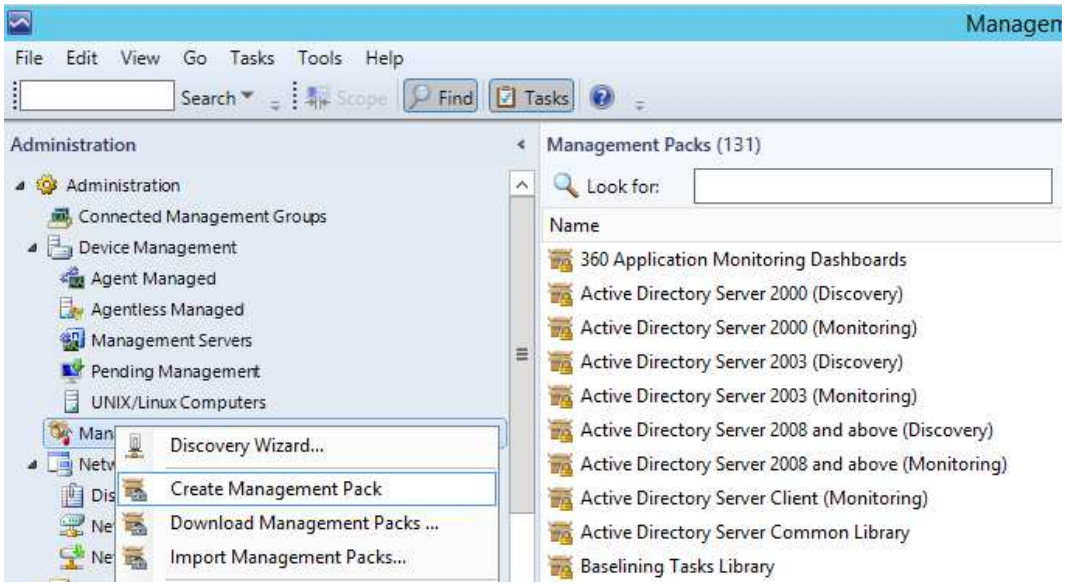


7. Kyseessä on AD-palvelin niin asetetaan agentti toimimaan välityspalvelimena. Tällöin agentti pystyy välittämään tietoa loogisista kokonaisuuksia kuten klustereista.

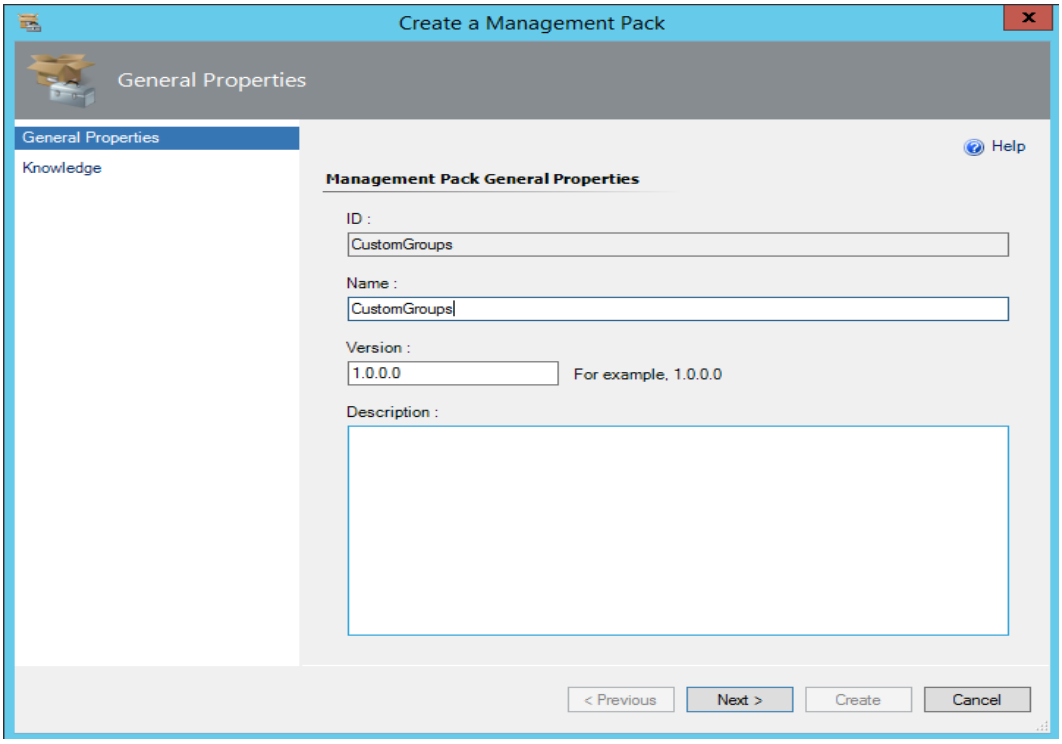


Liite 7. SCOM 2012 R2: oman ryhmän luominen

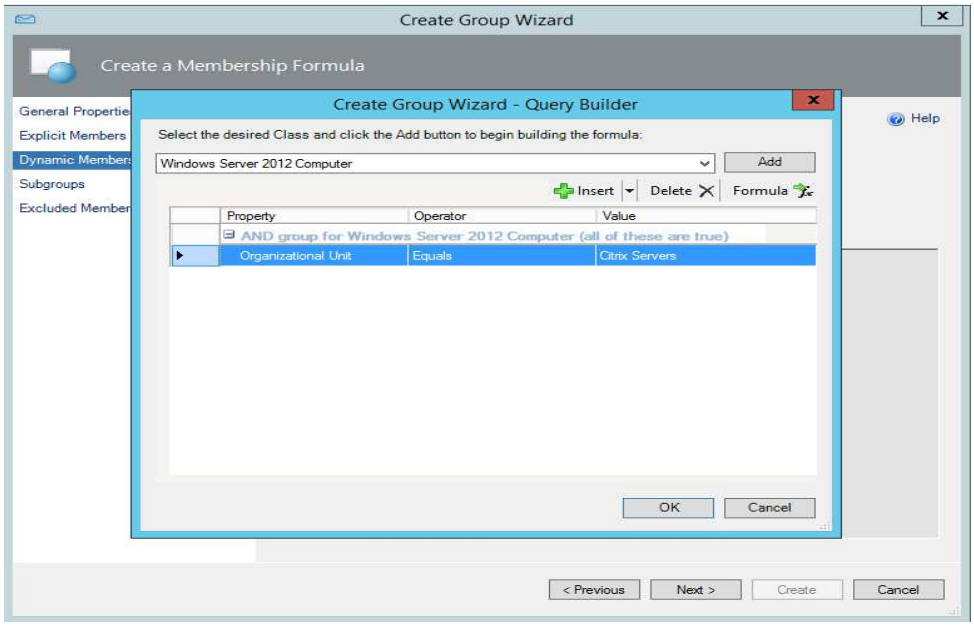
1. Aloitetaan luomalla oma hallintapaketti mukautetuille ryhmille.



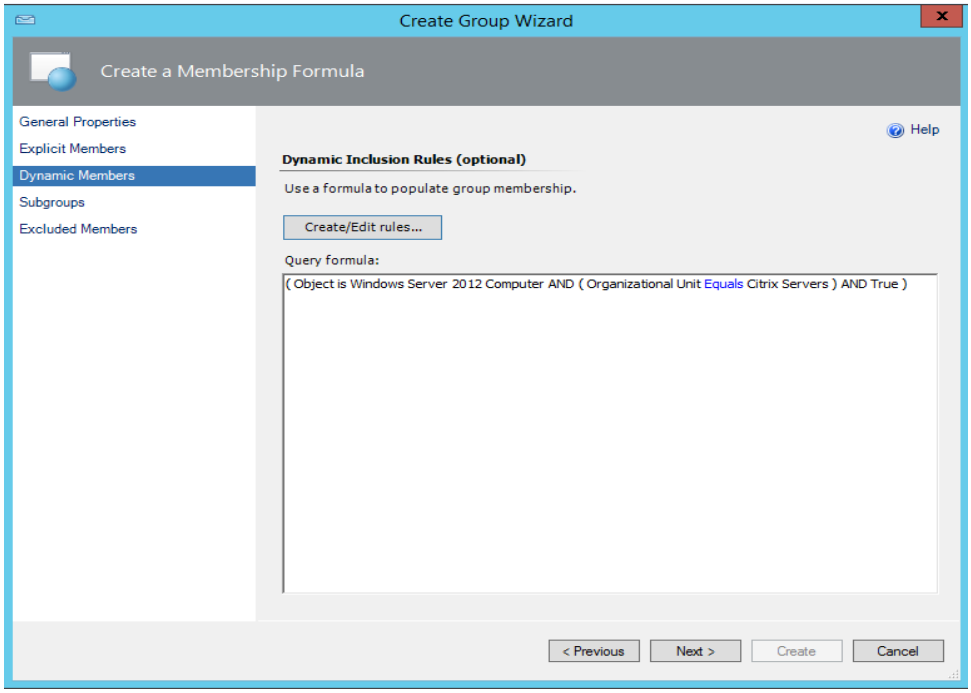
2. Nimetään hallintapaketti ja annetaan sille kuvaus.



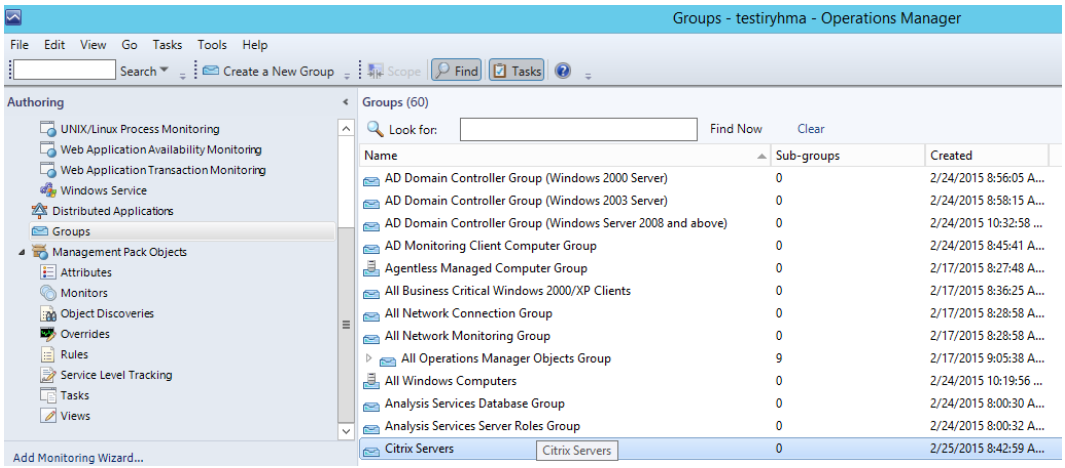
3. Luodaan esimerkkinä dynaaminen mukautettu ryhmä, jossa voidaan seurata kaikkia Citrix-palvelimia. Valitaan luokasta kaikki Windows 2012 palvelinkoneet ja määritetään kaikki Active Directoryn Citrix Servers Organizational Unitiin kuuluvat tietokoneet kuulumaan ryhmään.



4. Seuraavaksi tarkastellaan luotua ehtoa, jolla kohteet lisätään Citrix Server -ryhmään ja edetään ryhmän luonnissa eteenpäin kunnes ryhmä on luotu.

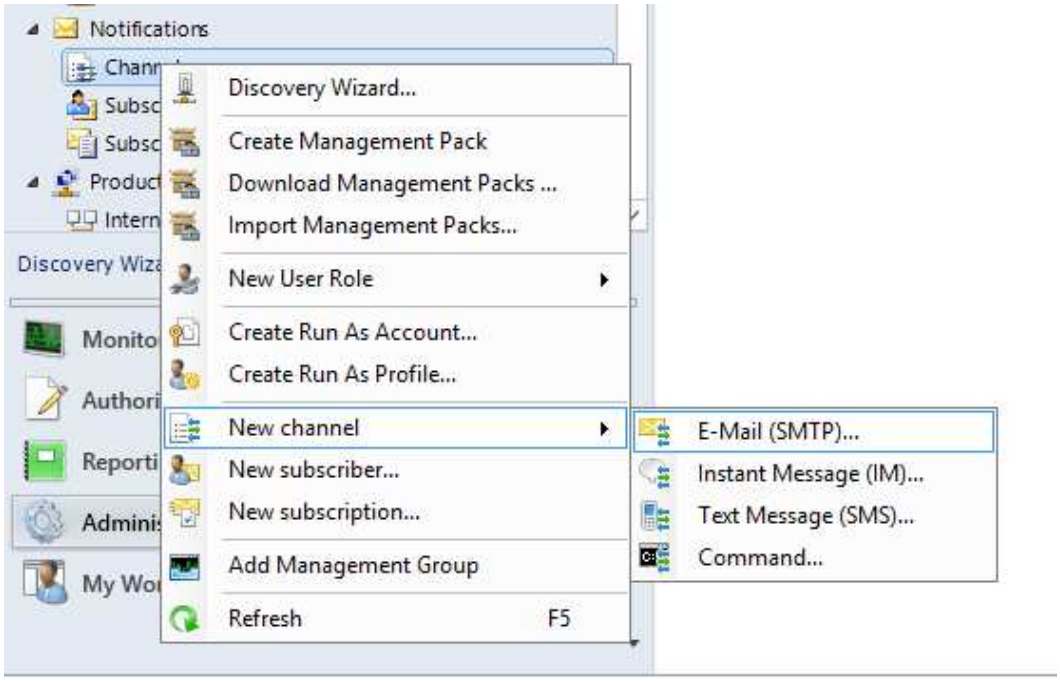


5.Dynaaminen mukautettu ryhmä on nyt luotu ja se voidaan havaita.

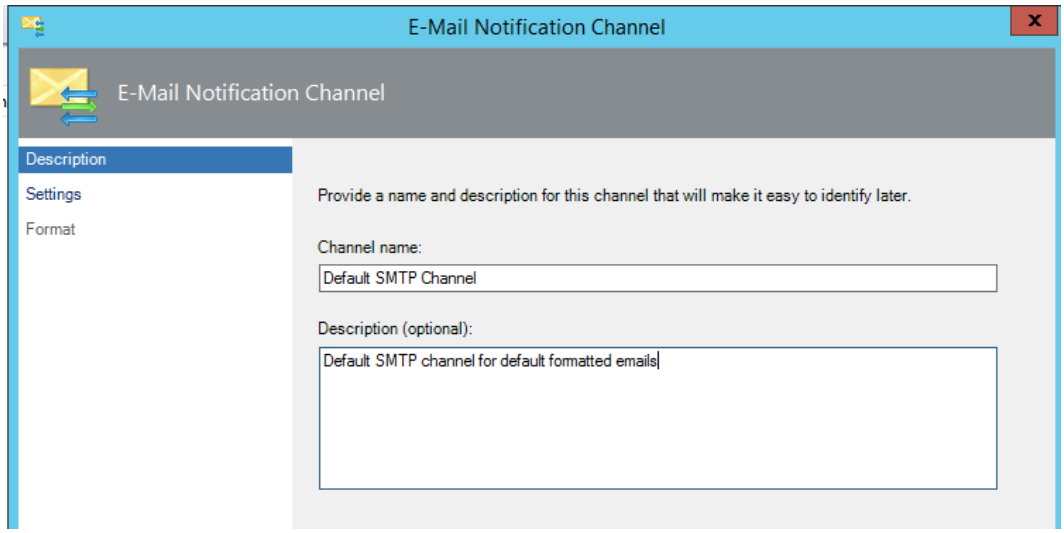


Liite 8. SCOM 2012 R2: hälytyksien ohjaus sähköpostiin

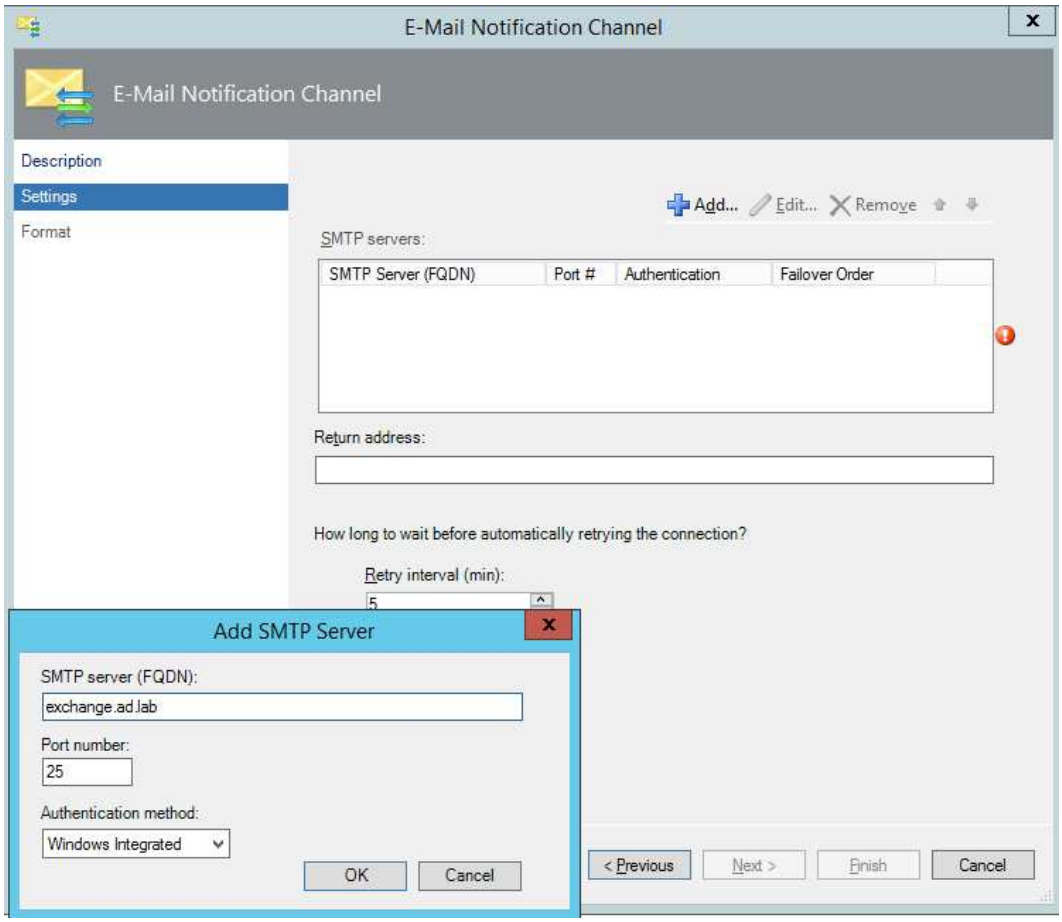
1. Aloitetaan luomalla sähköpostiviesteille oma kanava.



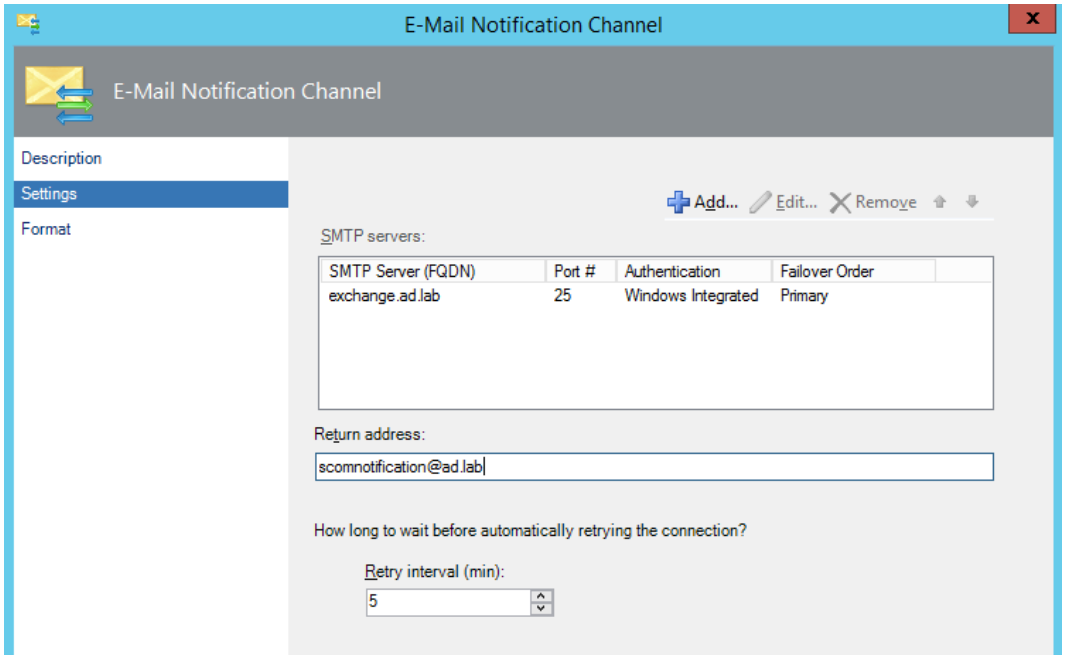
2. Nimetään seuraavaksi sähköpostille luotu kanava.



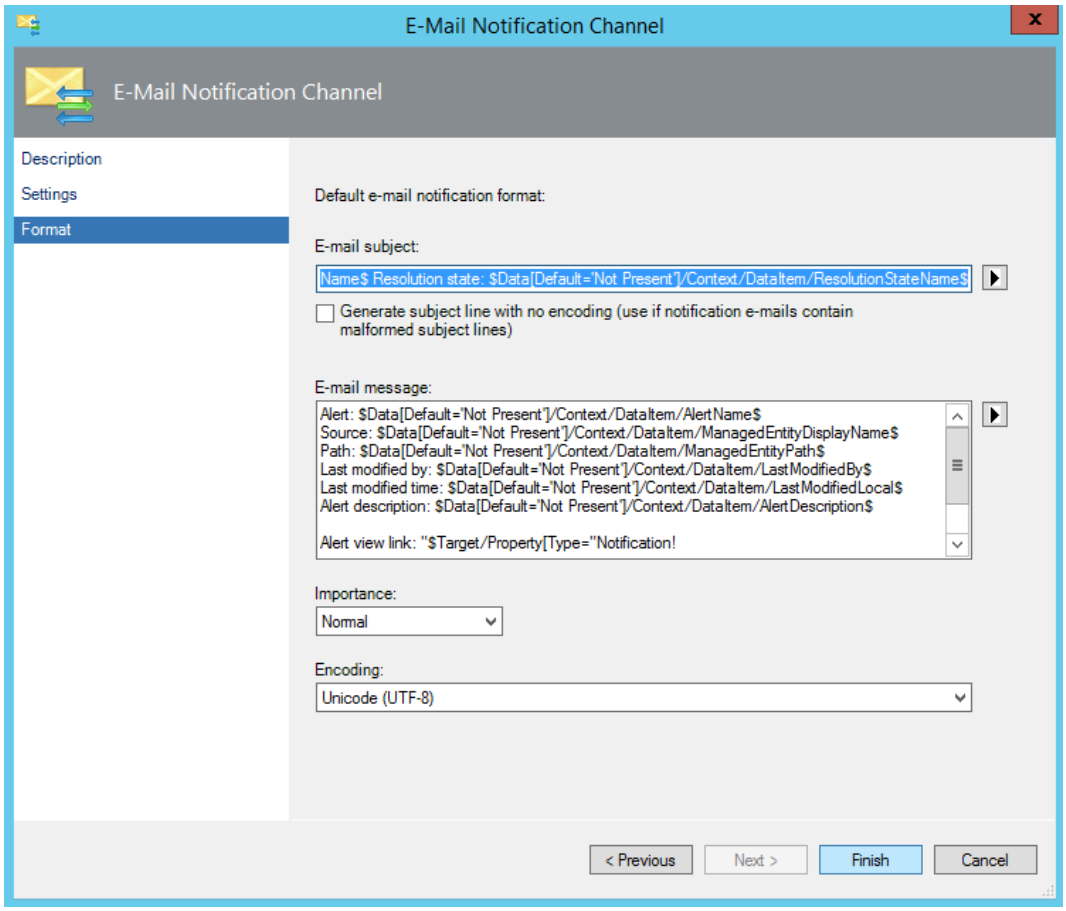
3. Lisätään sähköpostipalvelin käyttäen FQDN ja määritetään käytettävä portti. Valitaan tunnistautumisvaihtoehdoksi Windows tunnistautuminen anonyymin sijasta.



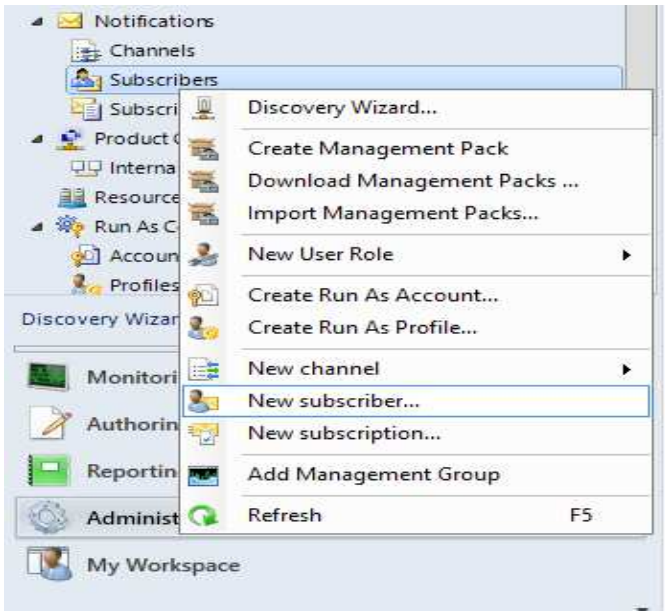
4. Sähköpostipalvelimen määrityksen jälkeen, määritetään return address.



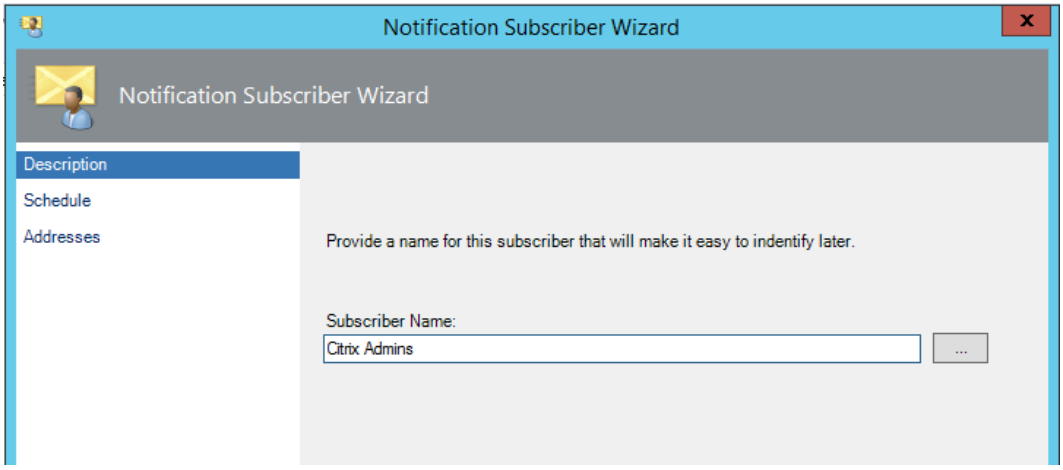
5. Lopuksi viestien muotoa on mahdollista muokata halutessaan.



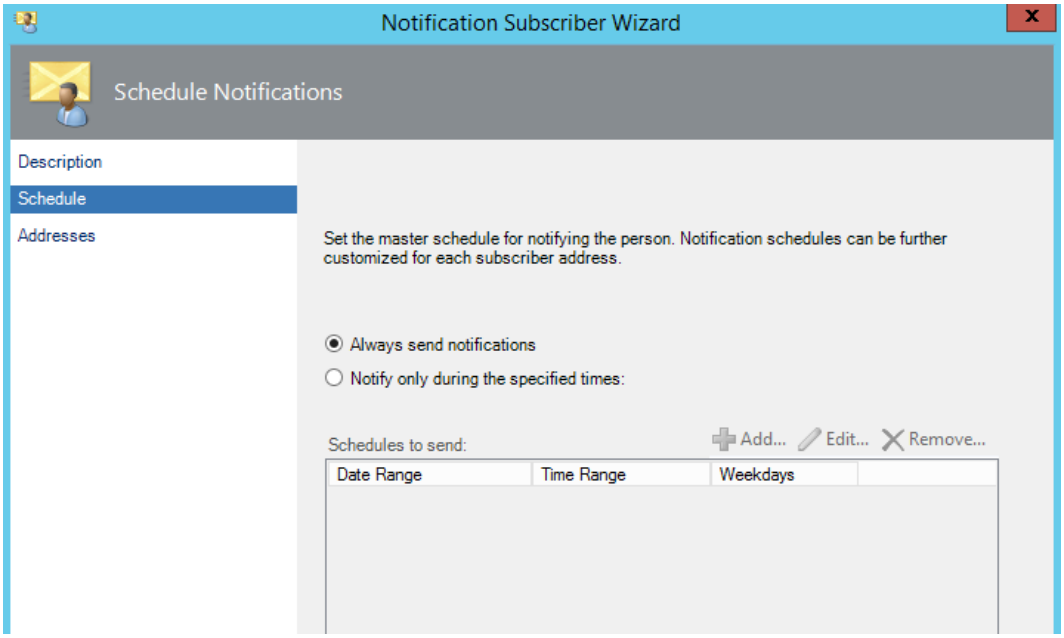
6. Määritetään luodulle kanavalle tilaajat (subscribers).



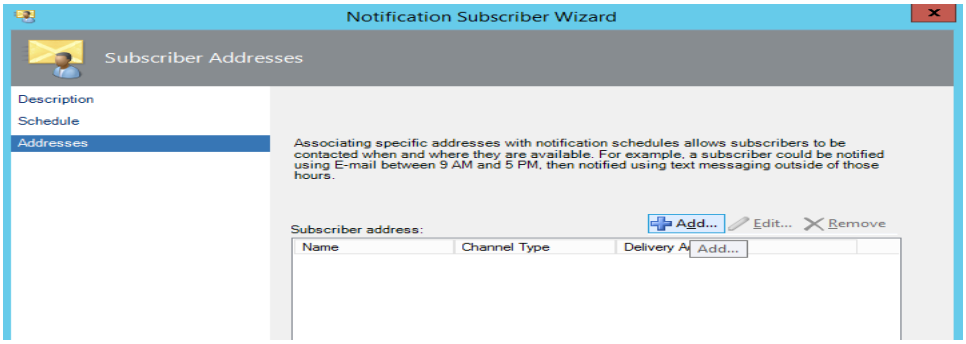
7. Seuraavaksi määritetään tilaajan nimi.



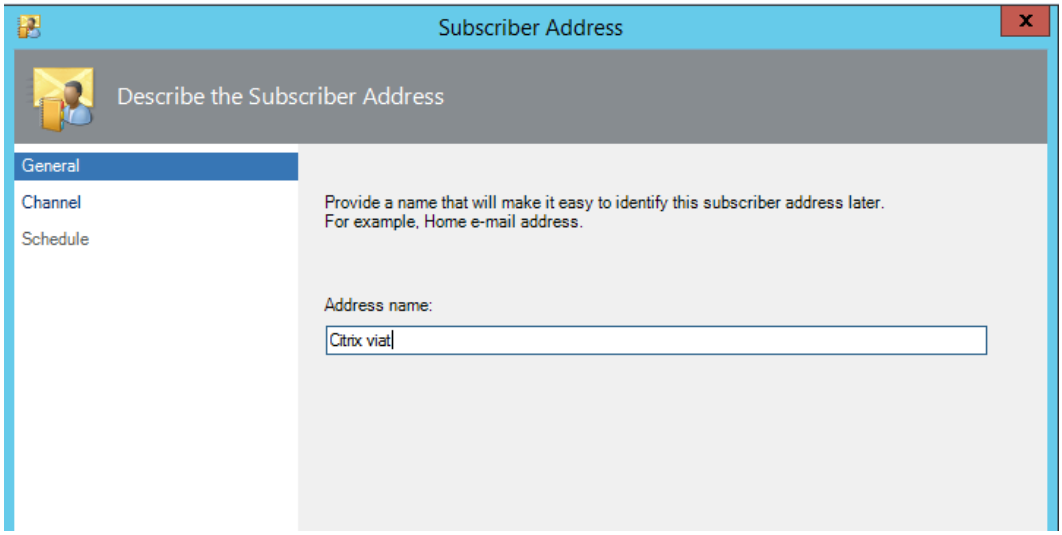
8. Määritetään viestienlähettämisaikataulu niin, että viestit lähetetään aina.



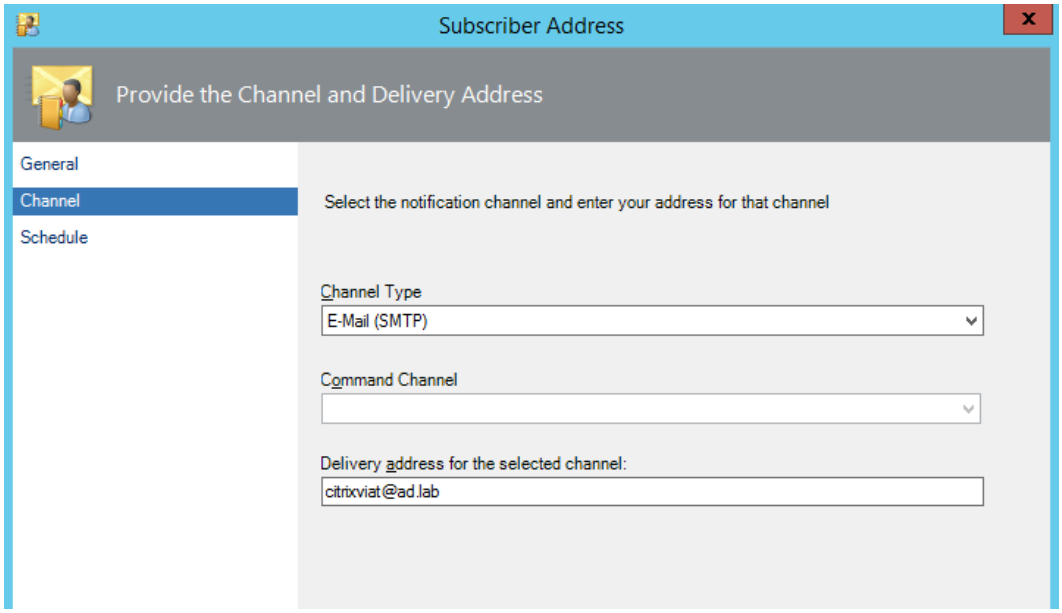
9. Lisätään seuraavaksi osoitteet, joihin halutaan viestit lähettää.



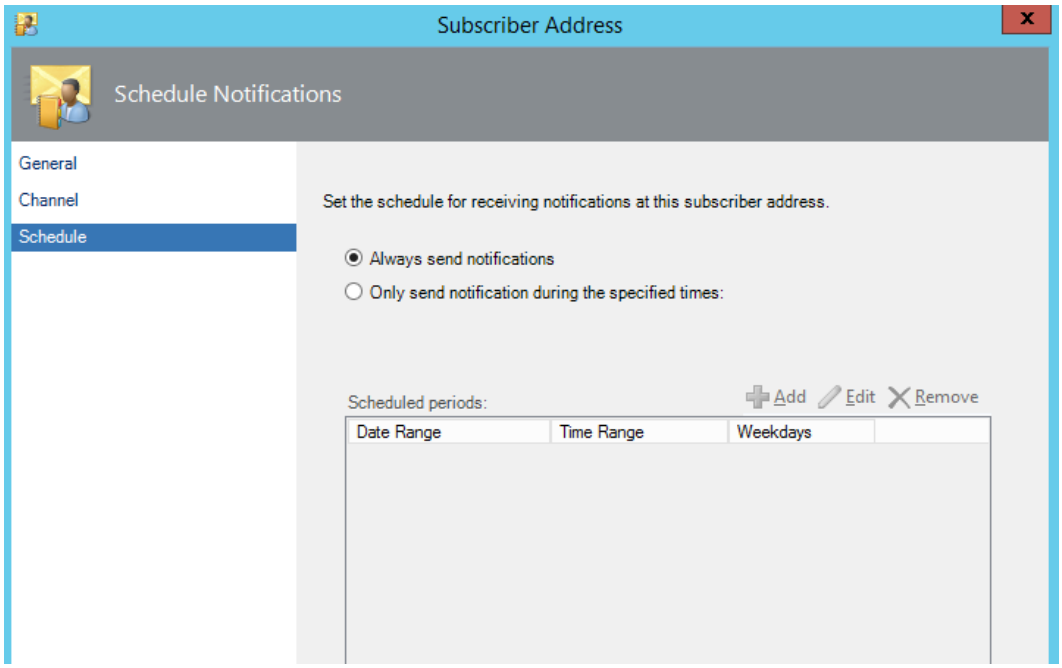
10. Seuraavaksi avautuu erillinen ikkuna, jossa voidaan määrittää tarkemmin tilaajan nimi ja muut tiedot.



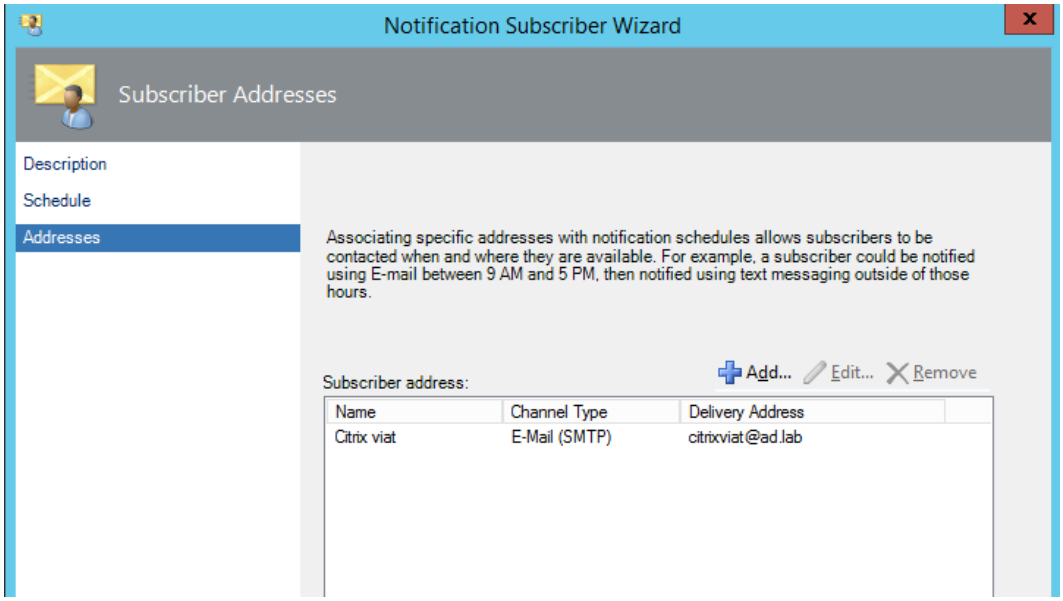
11. Valitaan kanava, joka luotiin aiemmin ja sidotaan se sähköpostiosoitteeseen / sähköpostilaatikkoon.



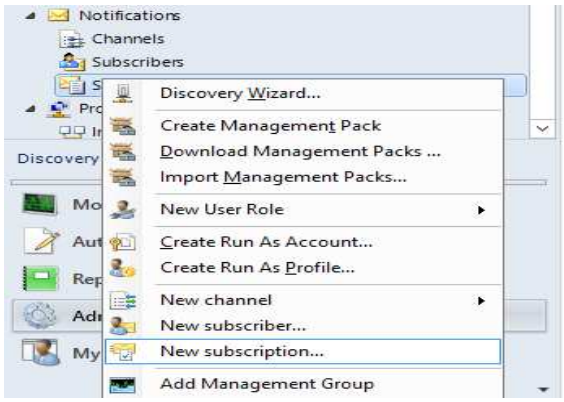
12. Määritetään jälleen lähetysaikataulu viesteille. Kyseinen aikataulu on käyttäjäkohtainen eli aiemmin luotu lähetysaikataulu on yleisesti Citrixin järjestelmäylläpitäjille.



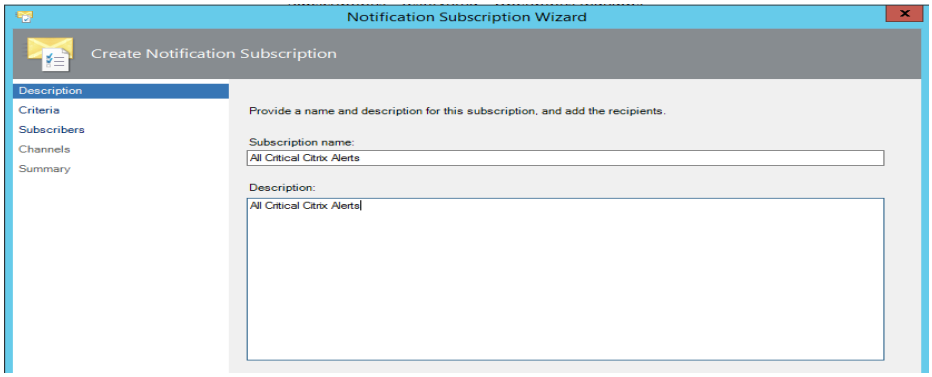
13. Lopuksi luodaan tilaaja ja tarkistetaan tehdyt määritykset.



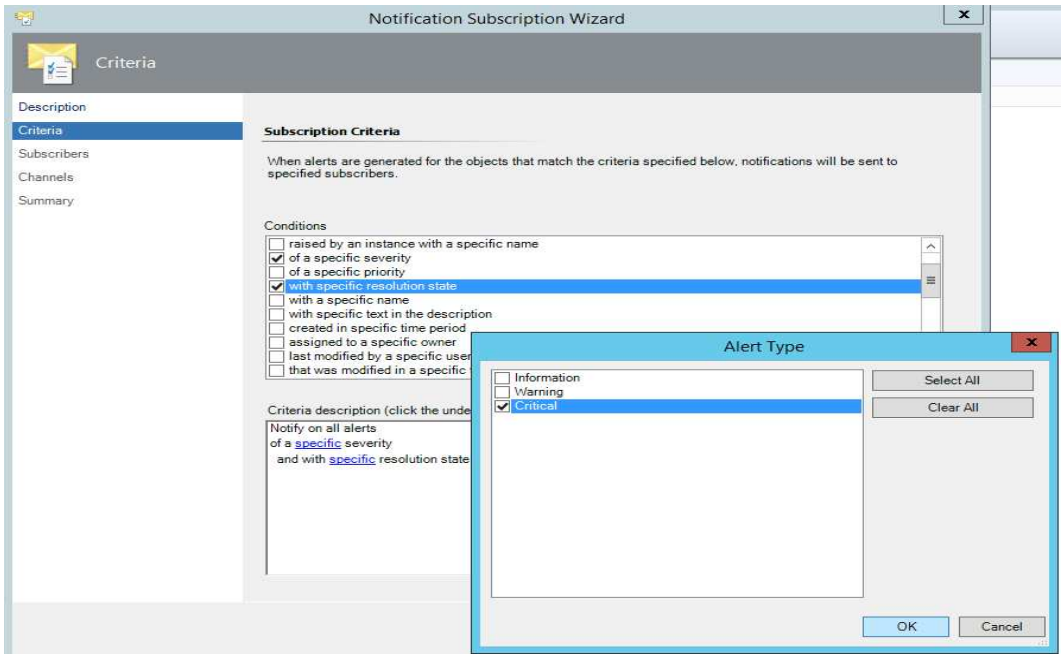
14.Kun kanava ja tilaaja ovat luotuna, SCOM:lle pitää luoda ehdot joiden täyttyessä viesti lähetetään tilaajalle.



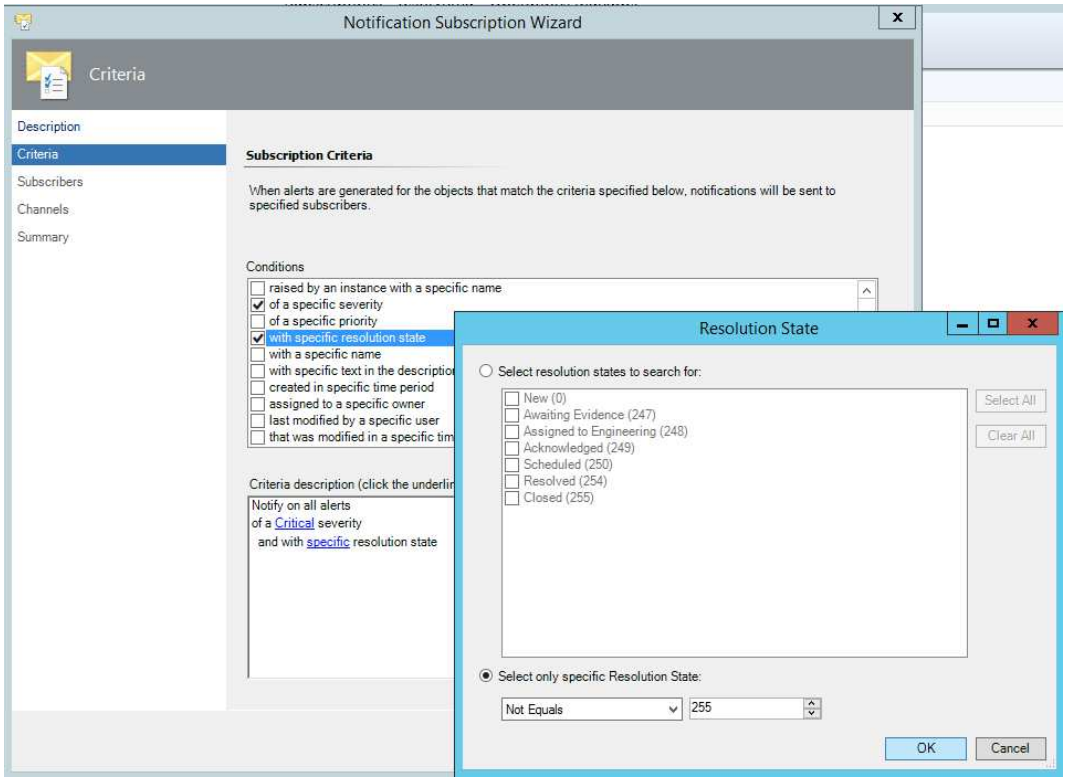
15. Määritetään nimi luodulle ennakkoehdoille.



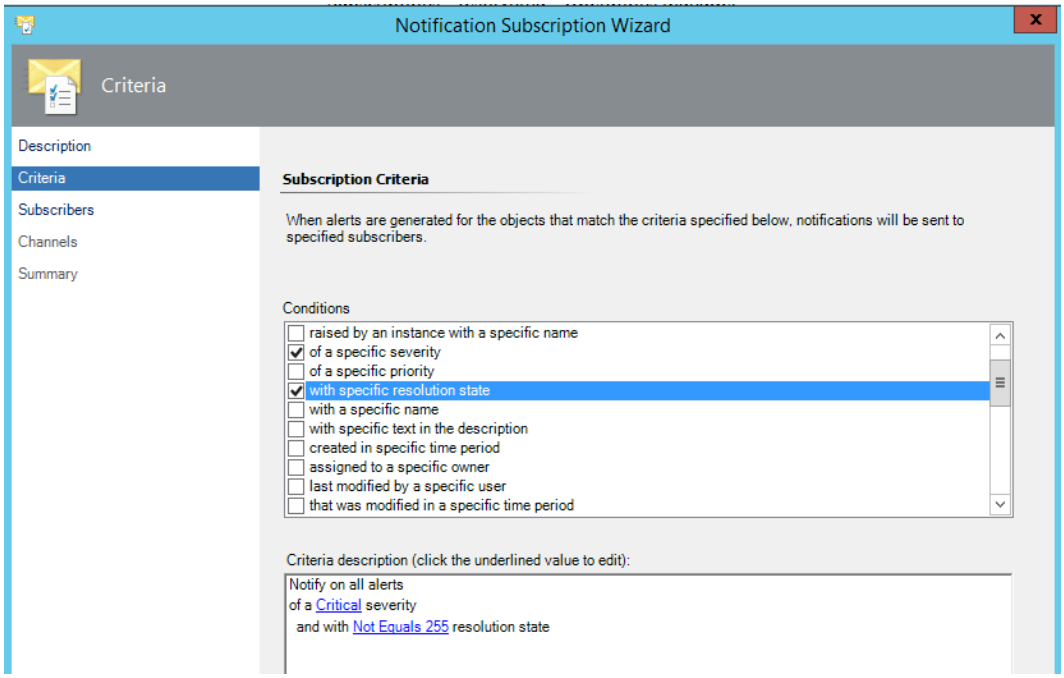
16. Seuraavaksi määritetään ehdot, joiden toteutuessa viesti lähetään tilaajalle. Valitaan ehdoiksi hälytyksen tyyppi ja tila. Määritetään hälytyksen vakavuudeksi kriittinen.



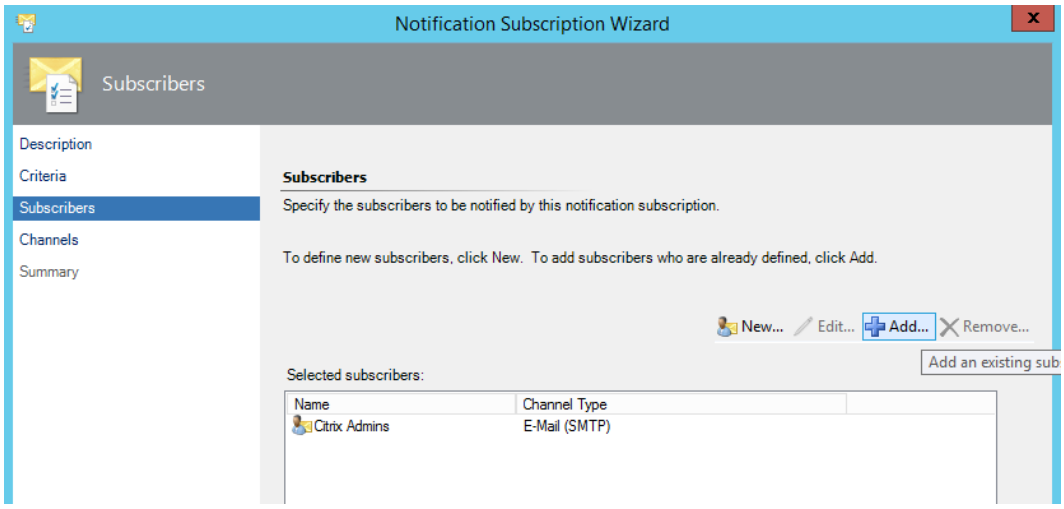
17. Määritetään vielä hälytyksen tila. Valitaan kaikki hälytykset, jotka eivät ole suljettuja eli niiden arvo on jokin muu kuin 255.



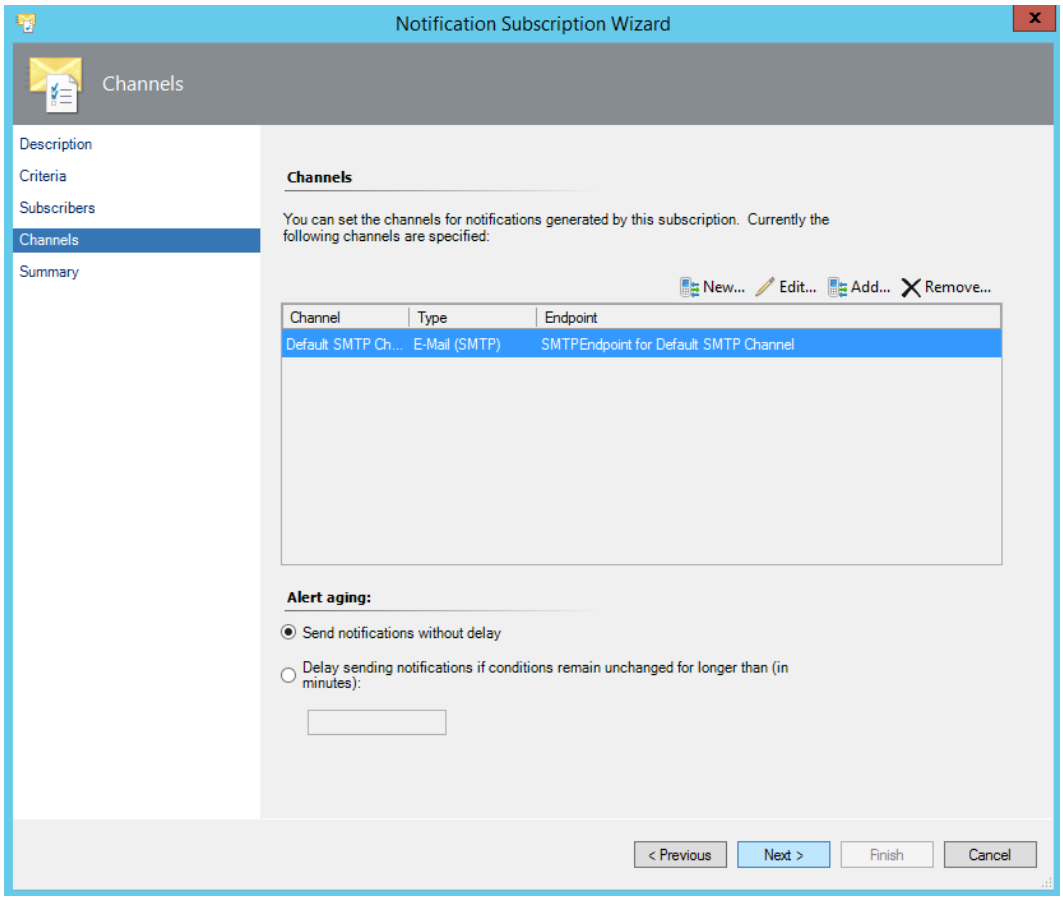
18. Varmistetaan vielä määritetyt ehdot. Hälytyksistä, jotka ovat vakavuudeltaan kriittisiä ja eivät ole suljettuja, ilmoitetaan tilaajalle.



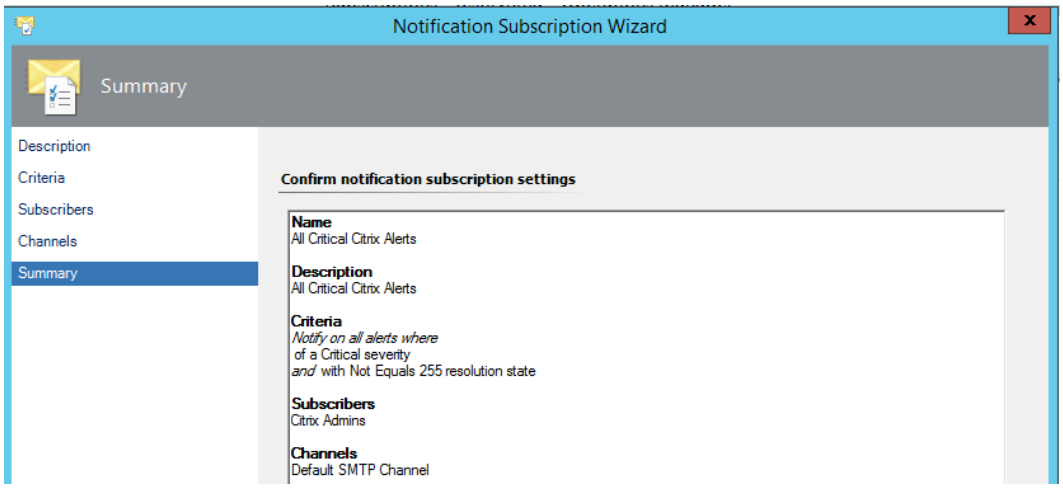
19.Ehtojen jälkeen valitaan tilaajat. Lisätään luotu Citrix Admins tilaaja.



20. Määritetään vielä kanava, jolla seuraavia ehtoja käytetään.



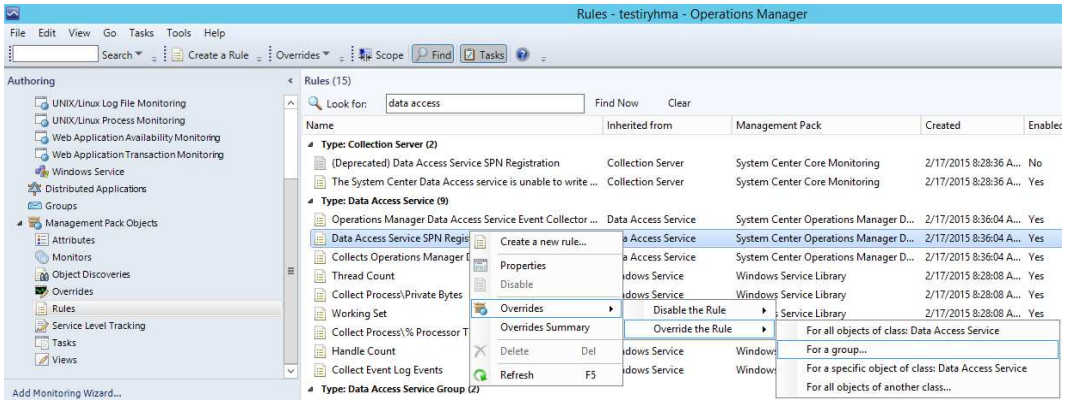
21. Ennen lopullista ehtojen luontia voidaan vielä tarkastella tehdyt määritykset ja hyväksyä ne.



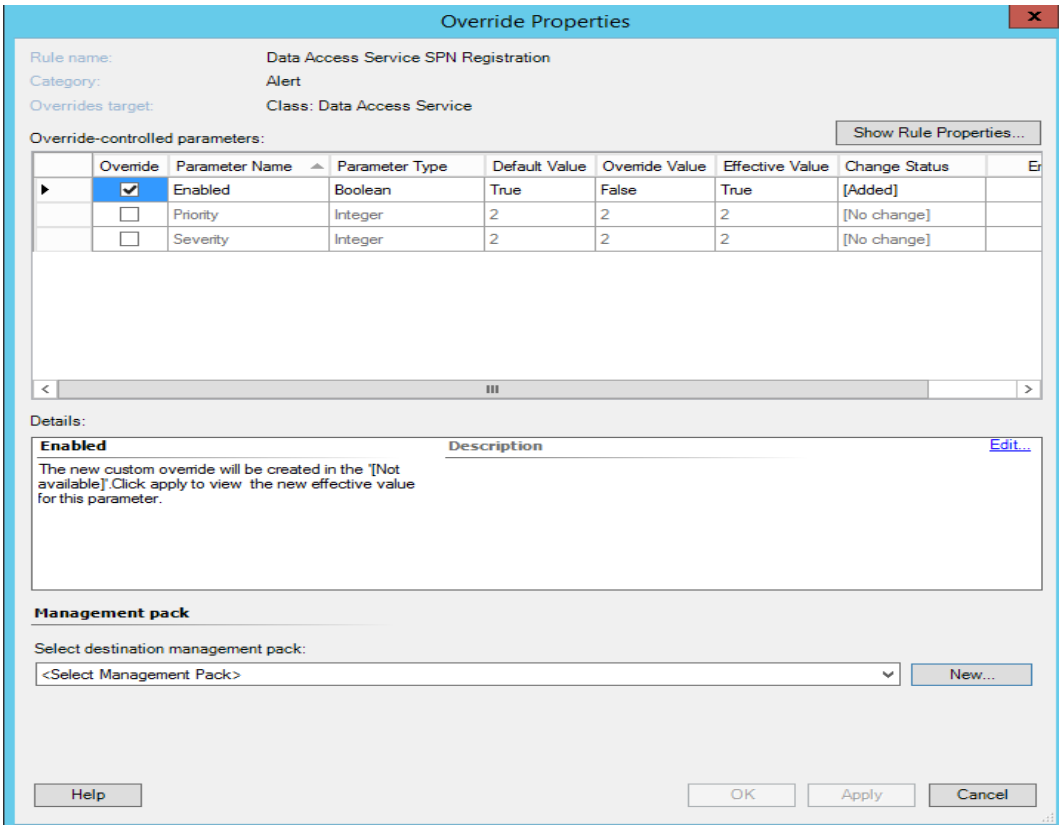
Kun kanava, tilaaja ja niihin sidotut ehdot ovat luotuna, ehdot täyttävistä hälytyksistä ilmoitetaan nyt sähköpostitse määritetyille tilaajille.

Liite 9. SCOM 2012: Overrides

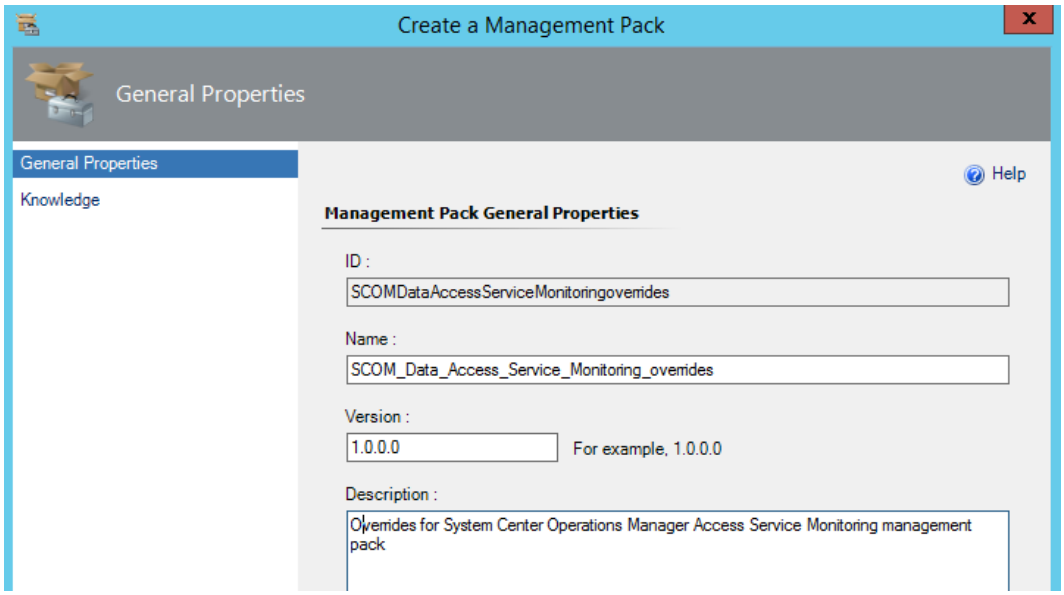
1. Virheelliseksi todettu hälytys, joka toistui jatkuvasti voidaan sivuuttaa menemällä navigaatiosta authoring valitsemalla rules. Sivuutetaan kyseinen sääntö koko ryhmältä.



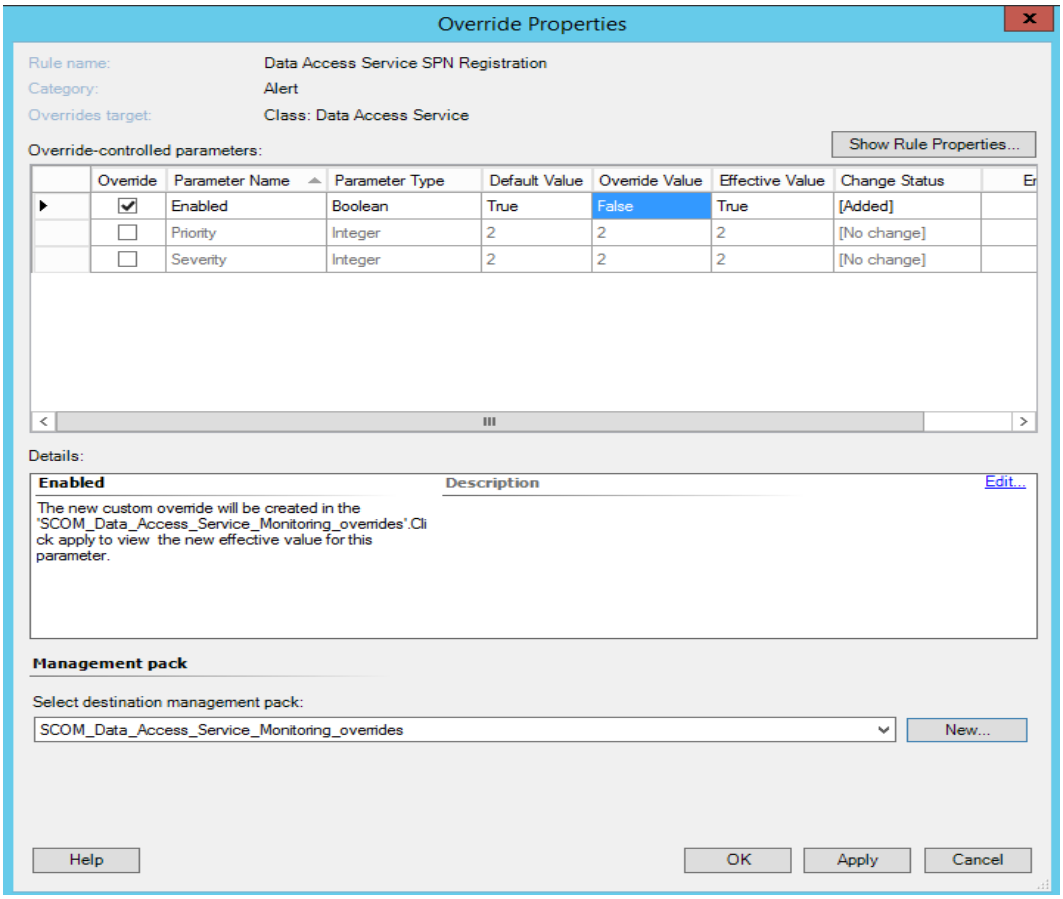
2. Valitaan override kohta ylhäältä ja määritetään override arvoksi false. Jos kyseessä olisi jokin attribuutti, sen arvoa voitaisiin halutessa muuttaa myös.



3. Luodaan uusi hallintapaketti / käytetään jo luotua hallintapakettia.

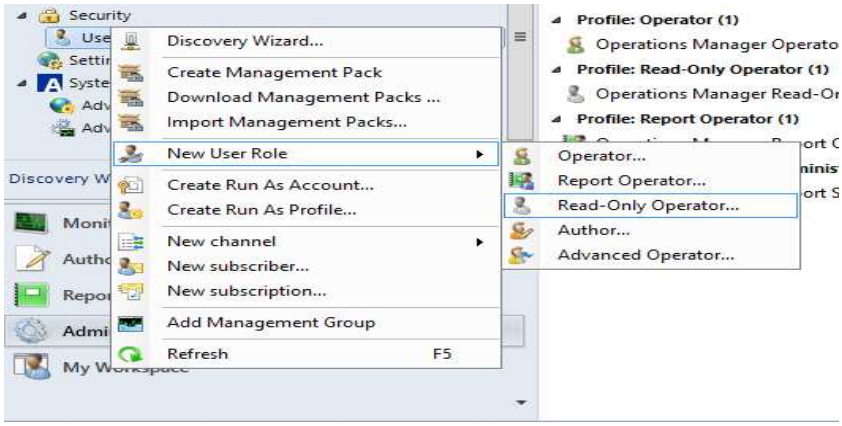


4. Nyt säännön sivuuttaminen voidaan ottaa käyttöön.

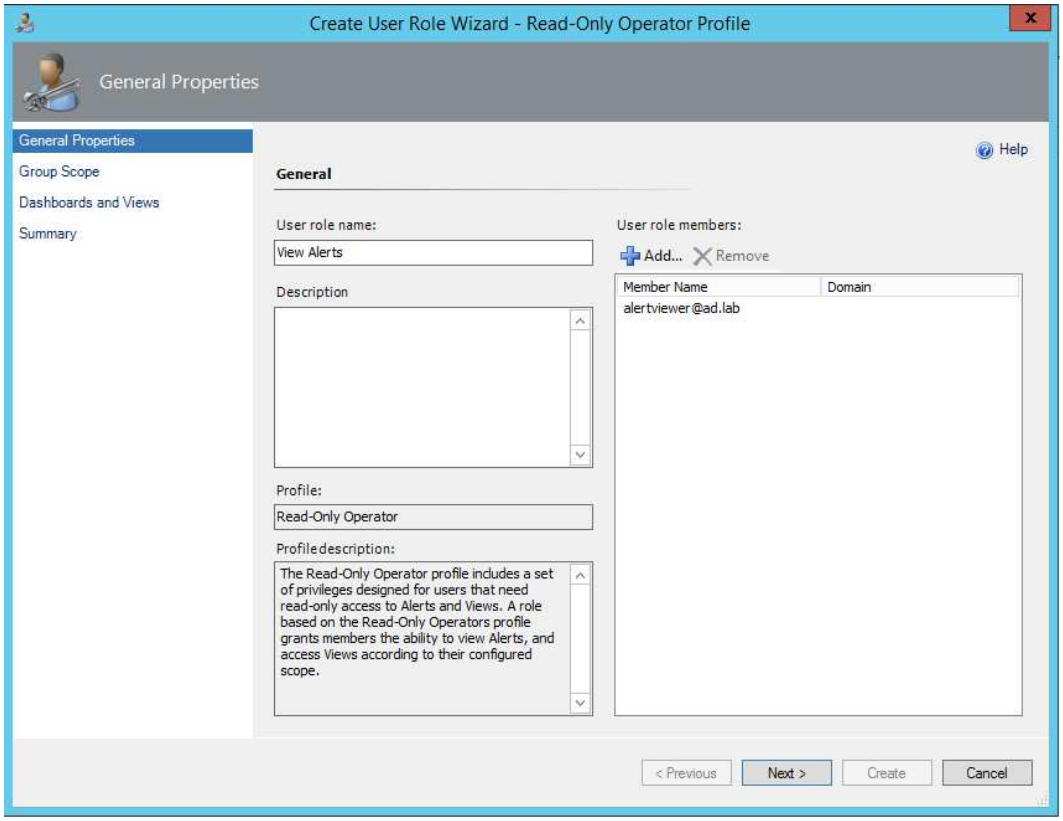


Liite 10. SCOM 2012 R2: käyttäjien luonti

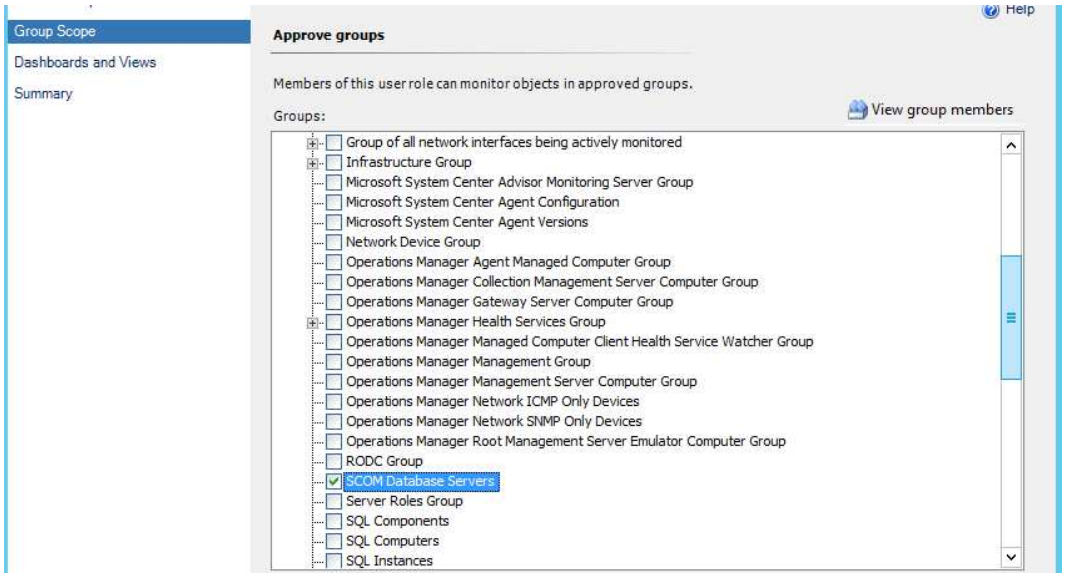
1. Valitaan uusi käyttäjärooli luotavaksi.



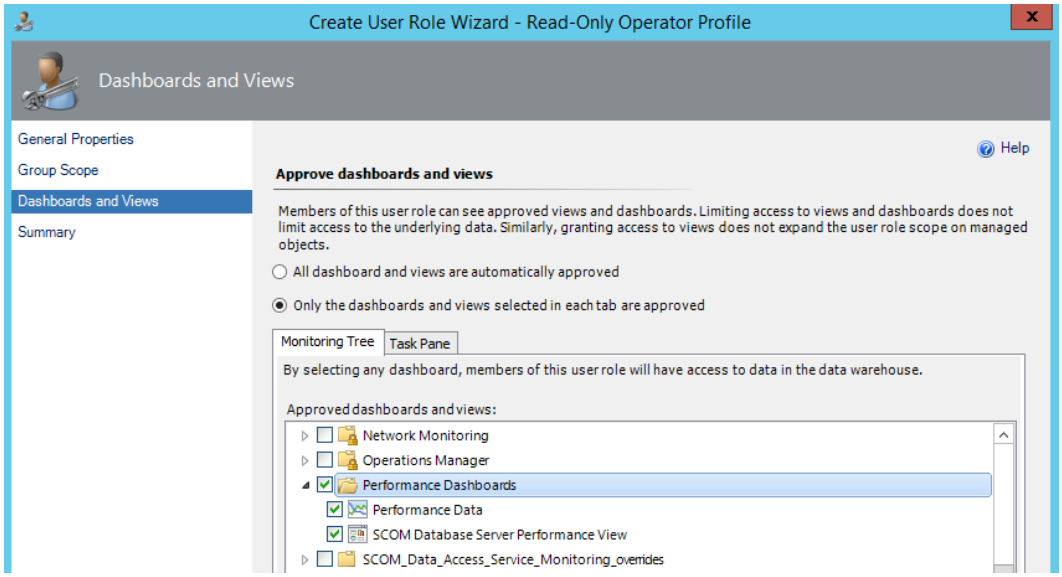
2. Luodaan käyttäjä, jolla oikeudet seurata meneillään olevia hälytyksiä.



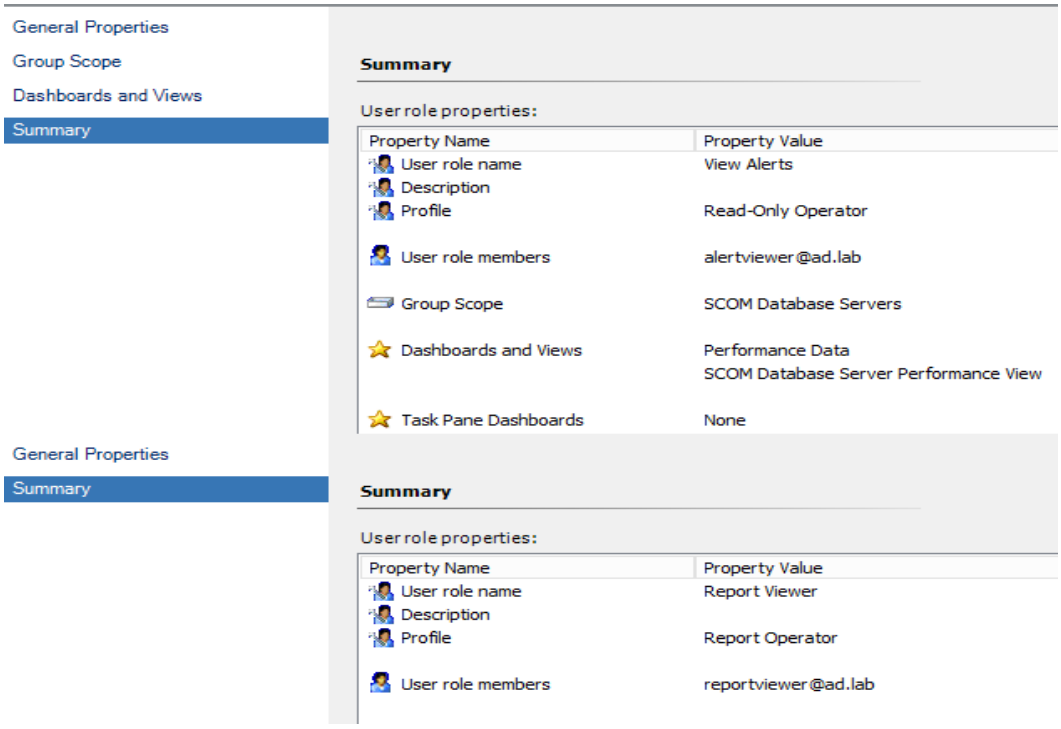
3. Seuraavaksi määritetään mihin käyttäjällä on oikeudet. Oikeudet voidaan rajata ryhmien mukaan ja rajataan oikeudet SCOM tietokantapalvelimiin.



4. Ryhmien lisäksi voidaan myös rajata käyttäjän näkemät näkymät. Käyttäjälle voidaan esimerkiksi luoda tiettyihin tarpeisiin sopivat näkymät, joihin oikeudet rajataan.

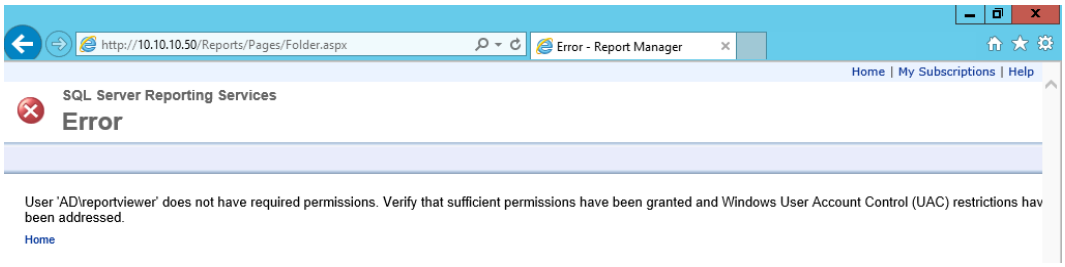


5. Nyt uusi käyttäjä voidaan luoda. Samalla tavalla voidaan myös luoda käyttäjä esimerkiksi raportointia varten.

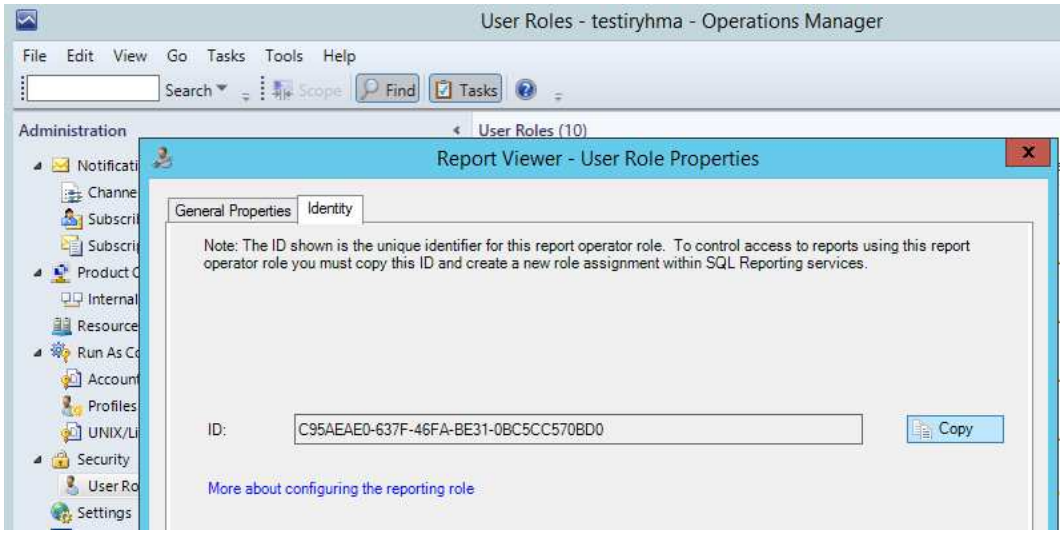


Liite 11. SCOM 2012 R2: raportointi

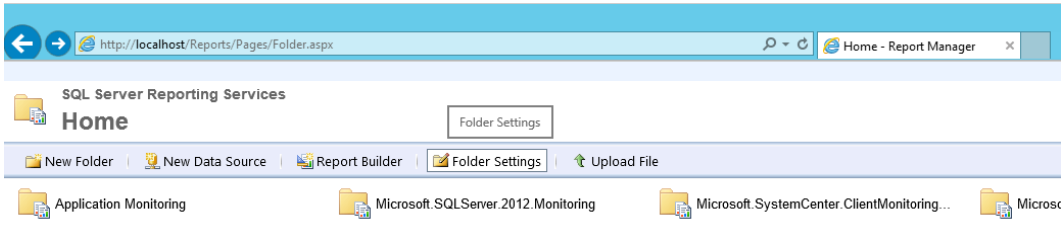
1. Raportteja voidaan lukea helposti selaimen avulla kirjautumalla raportointipalvelimelle. Luodulla käyttäjällä alertviewer ei ole oikeuksia, joten ne lisätään jälkeenpäin.



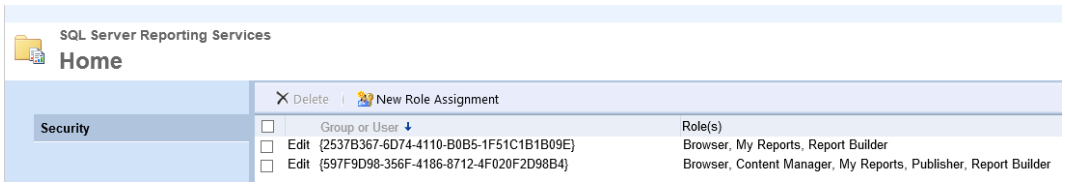
2. Käyttäjän oikeudet voidaan lisätä kopioimalla käyttäjän reportviewer ID ja lisäämällä uusi käyttäjä kyseisellä ID:llä raportointipalvelimelle.



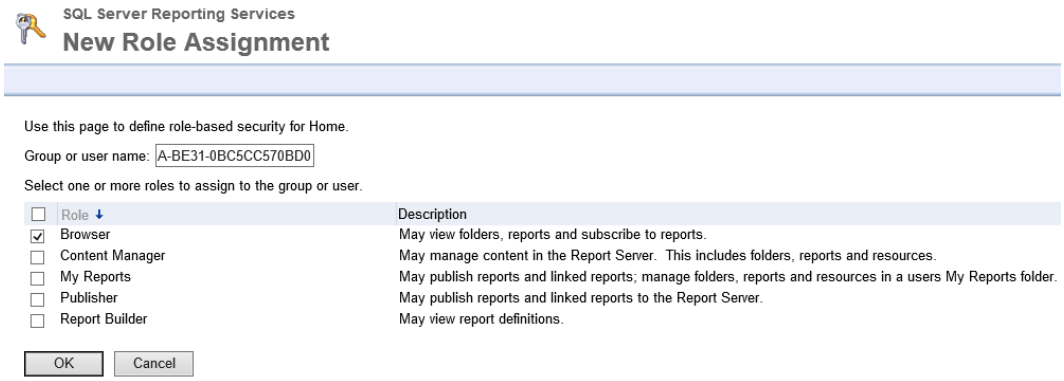
3. Kirjaudutaan raportointipalvelimelle järjestelmäylläpitäjänä ja lisätään käyttäjä valitsemalla ensin hakemiston asetukset.



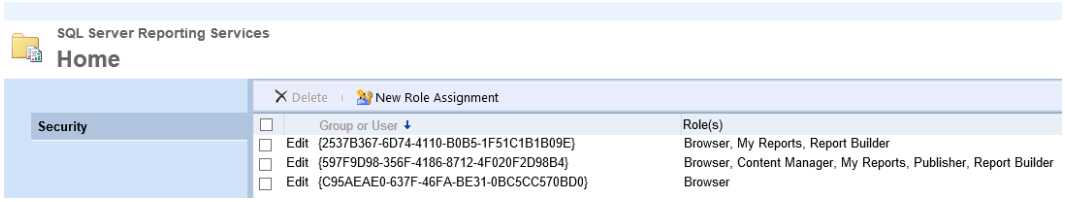
4. Valitaan uusi käyttäjärooli raportointipalvelimelle.



5. Liitetään seuraavaksi kopioitu reportviewer käyttäjä ID, raportointipalvelimelle luodulle käyttäjäroolille ja määritetään roolin oikeudeksi selaaja.

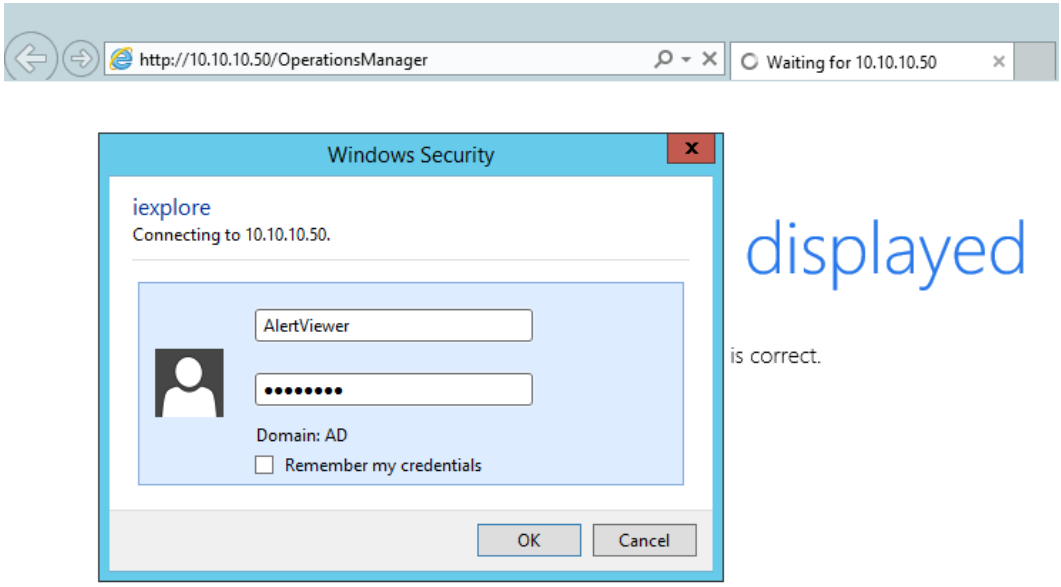


6. Nyt kun uudelle käyttäjälle on määritelty rooli sekä liitetty SCOM 2012 R2 käyttäjän ID pystyy kyseinen käyttäjä kirjautumaan raportointipalvelimelle onnistuneesti ja selaamaan raportteja selaimellaan.

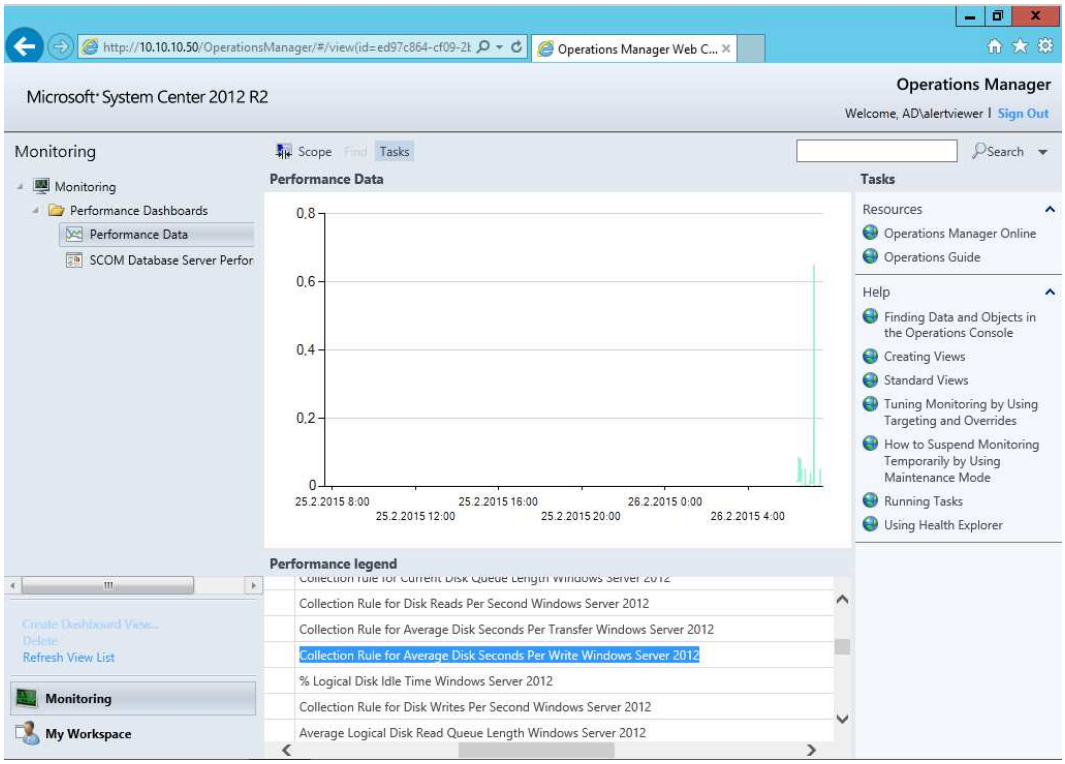


Liite 12. SCOM 2012 R2: Web Console

1. Kirjaudutaan hallintapalvelimelle hälytysten seurantaan luodulla käyttäjätunnuksella: alertviewer.

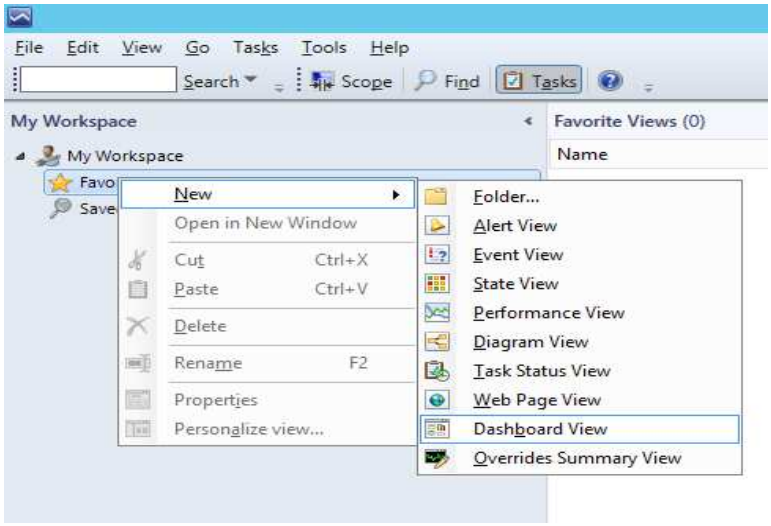


2. Käyttäjälle alertviewer mahdollistetaan näkyväksi aiemmin määritellyt ryhmät ja näkymät. Myöhemmin tarvittaessa lisää mukautettuja näkymiä voidaan lisätä tai ryhmiä.

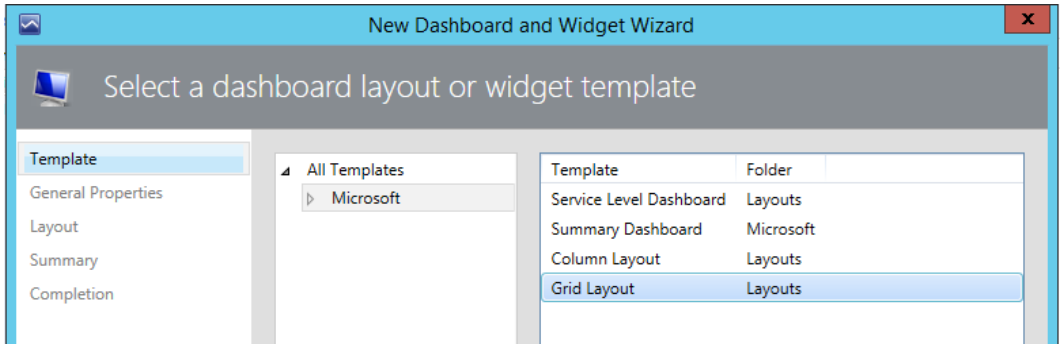


Liite 13. SCOM 2012 R2: mukautetun näkymän luominen

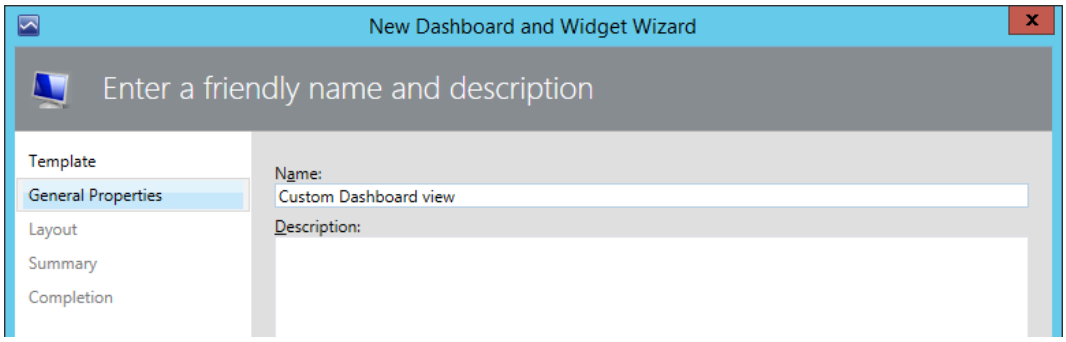
1. Luodaan seuraavaksi oma dashboard-näkymä.



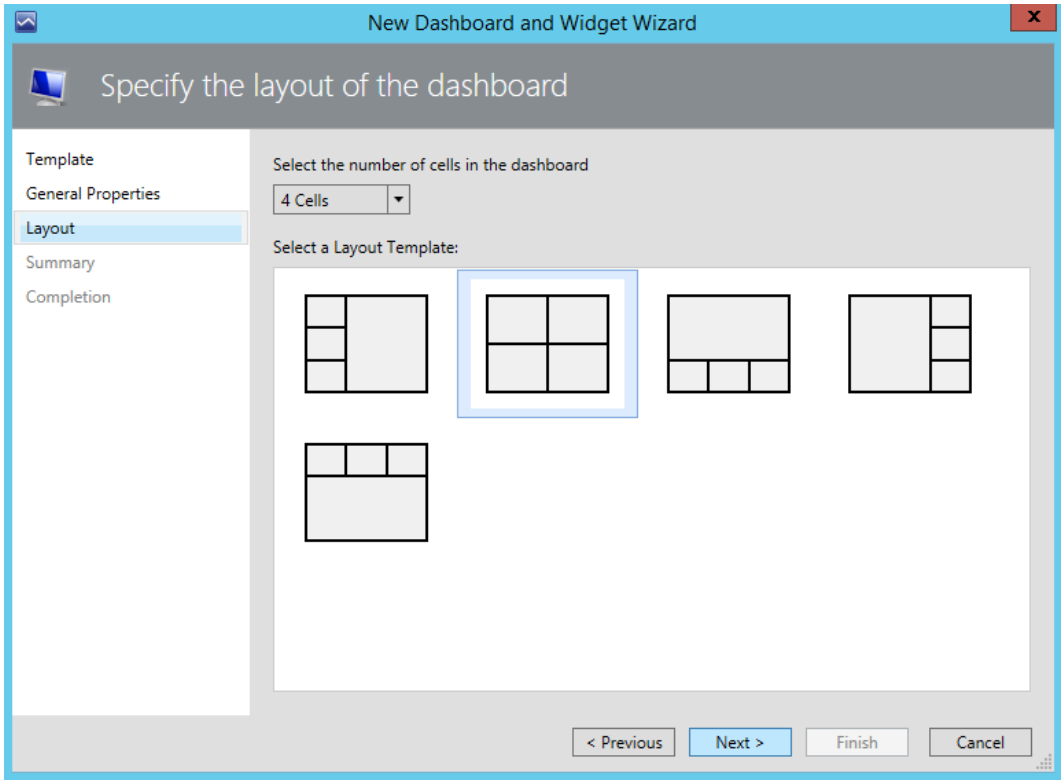
2. Valitaan näkymäksi valmis taulukkomainen pohja.



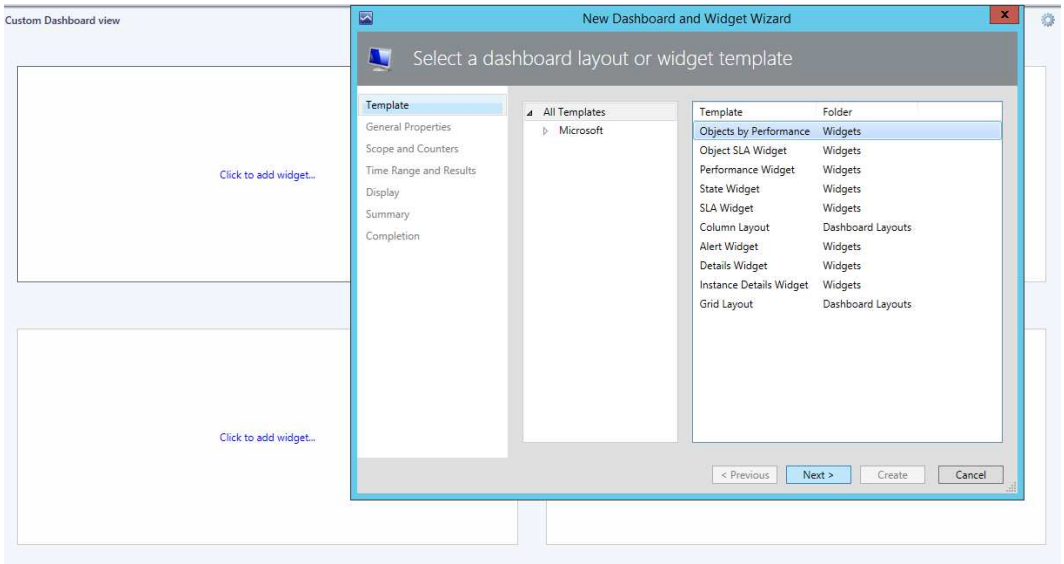
3. Määritetään luodulle näkymälle kuvaava nimi.



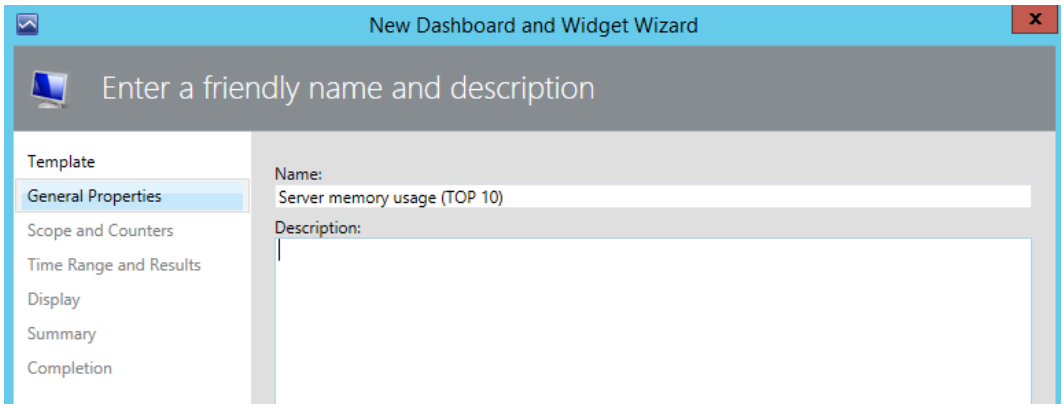
4. Valitaan omaan tarkoituksiin sopiva rakenne. Käytetään neljän solun pohjaa näkymässä.



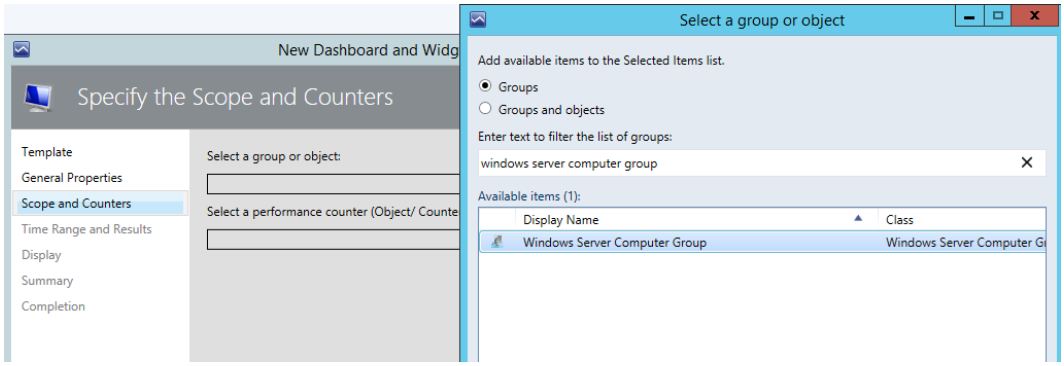
5. Luodaan lopuksi neljän solun taulukko johon, jokaiseen soluun voidaan lisätä muokattuja pienoisnäkymiä.. Valitaan yksi soluista ja lisätään pienoisnäkymä. Valitaan objects by performance.



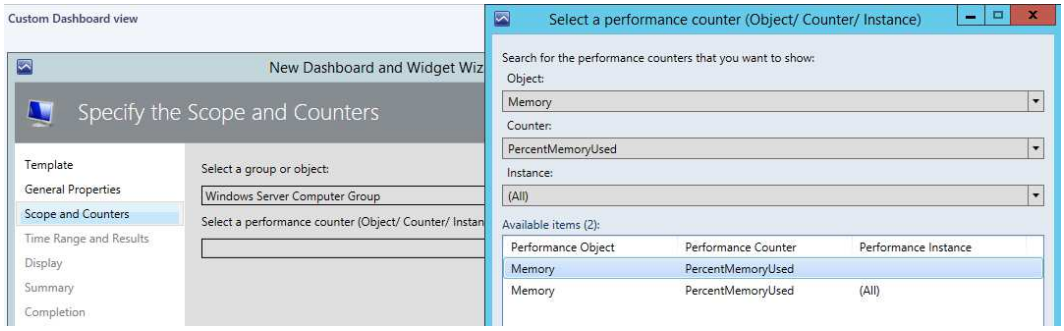
6.Valitaan kuvaava nimi uudelle pienoisnäkymälle.



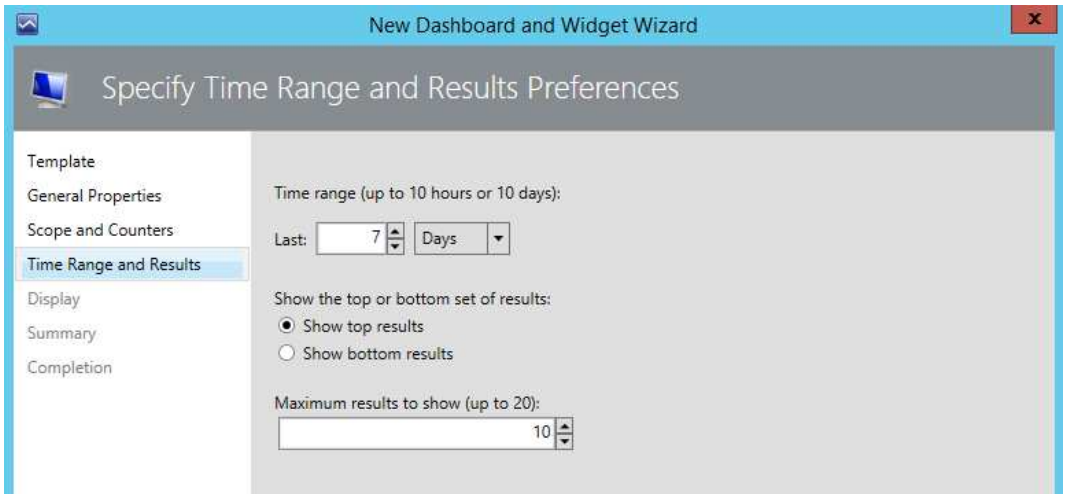
7. Seuraavaksi valitaan ryhmät tai kohteet, joita halutaan valvoa.



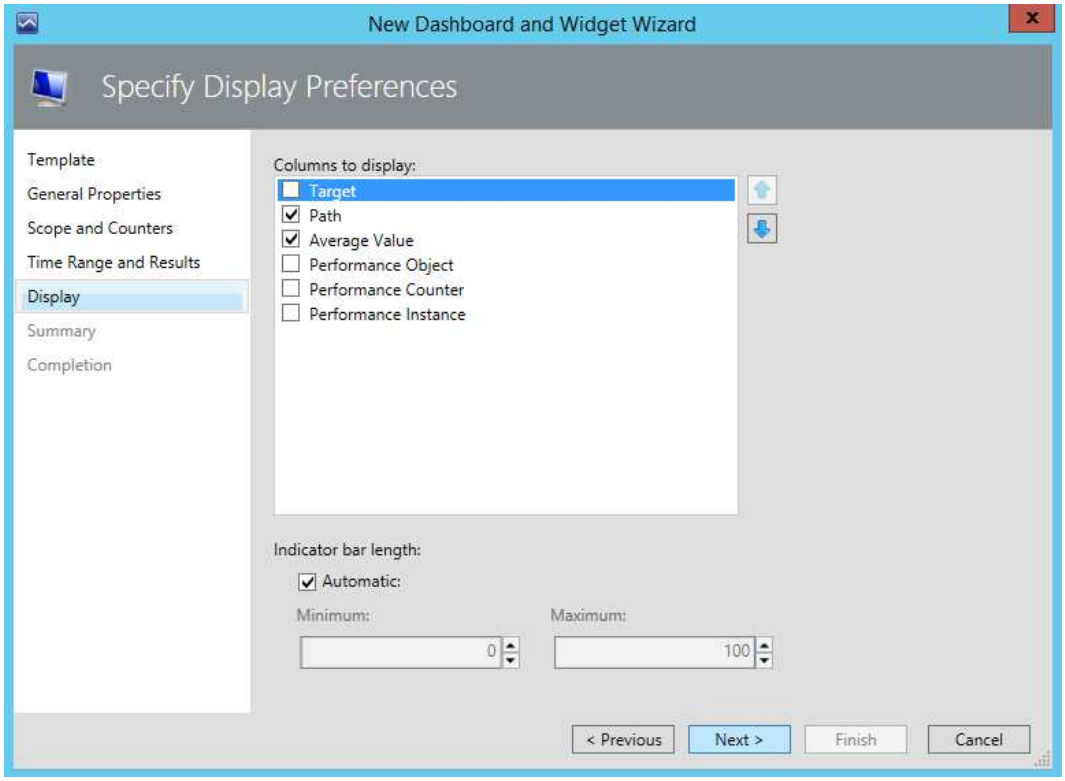
8. Valitaan kohteeksi muisti ja laskuriksi, kuinka paljon muistia on käytettynä.



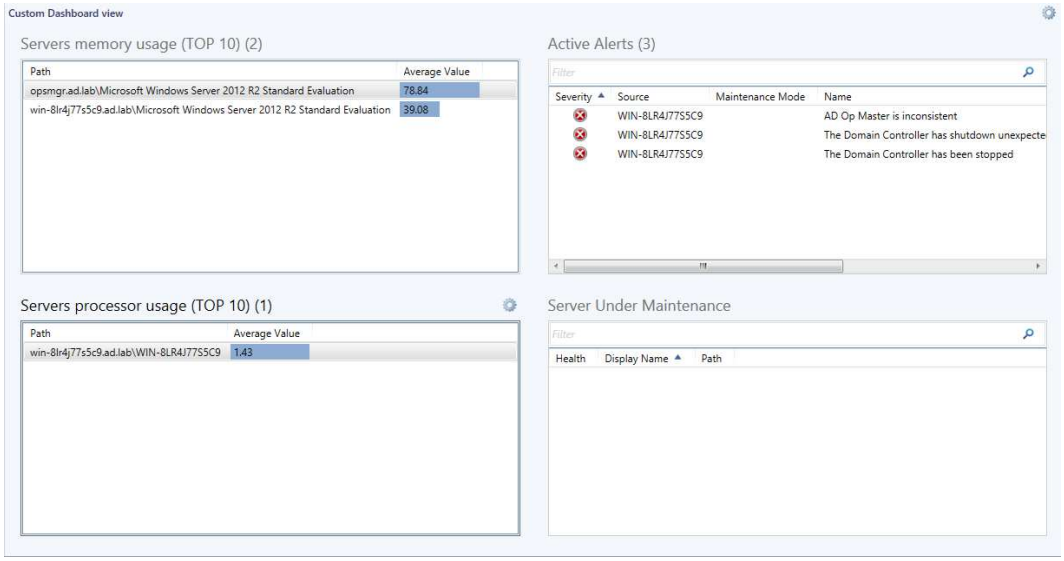
9. Määritetään näytettäväksi viimeisen viikon sisältä palvelimien muistinkäyttö. Määritetään myös näytettäväksi korkeimmat tulokset ja kymmenestä kohteesta.



10. Lopuksi määritetään mitä näytetään pienoisnäkymässä. Poisluetaan kohde kohta, koska se vie tilaa liikaa pienoisnäkymästä ja vaikeuttaa tarkastelua. Valitaan näytettäväksi polku ja keskimääräinen arvo.

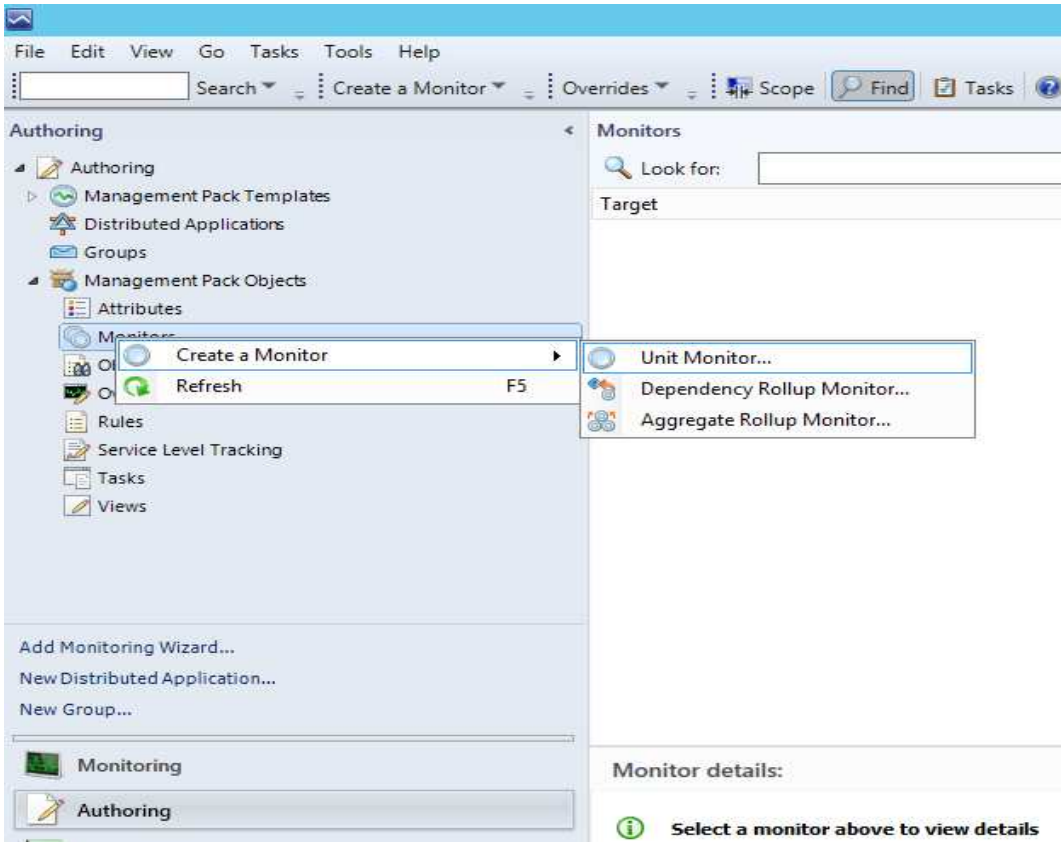


11. Lopuksi voidaan tarkastella luotua pienoisnäkymää ja sen tuloksia. Kokonaisnäkymään on lisätty myös muutama pienoisnäkymä.

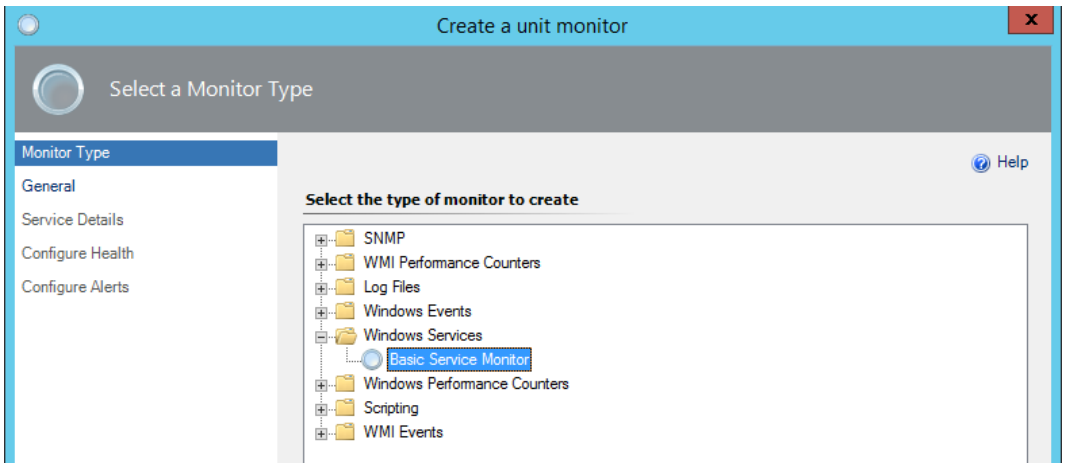


Liite 14. SCOM 2012 R2: palvelun automaattinen käynnistäminen

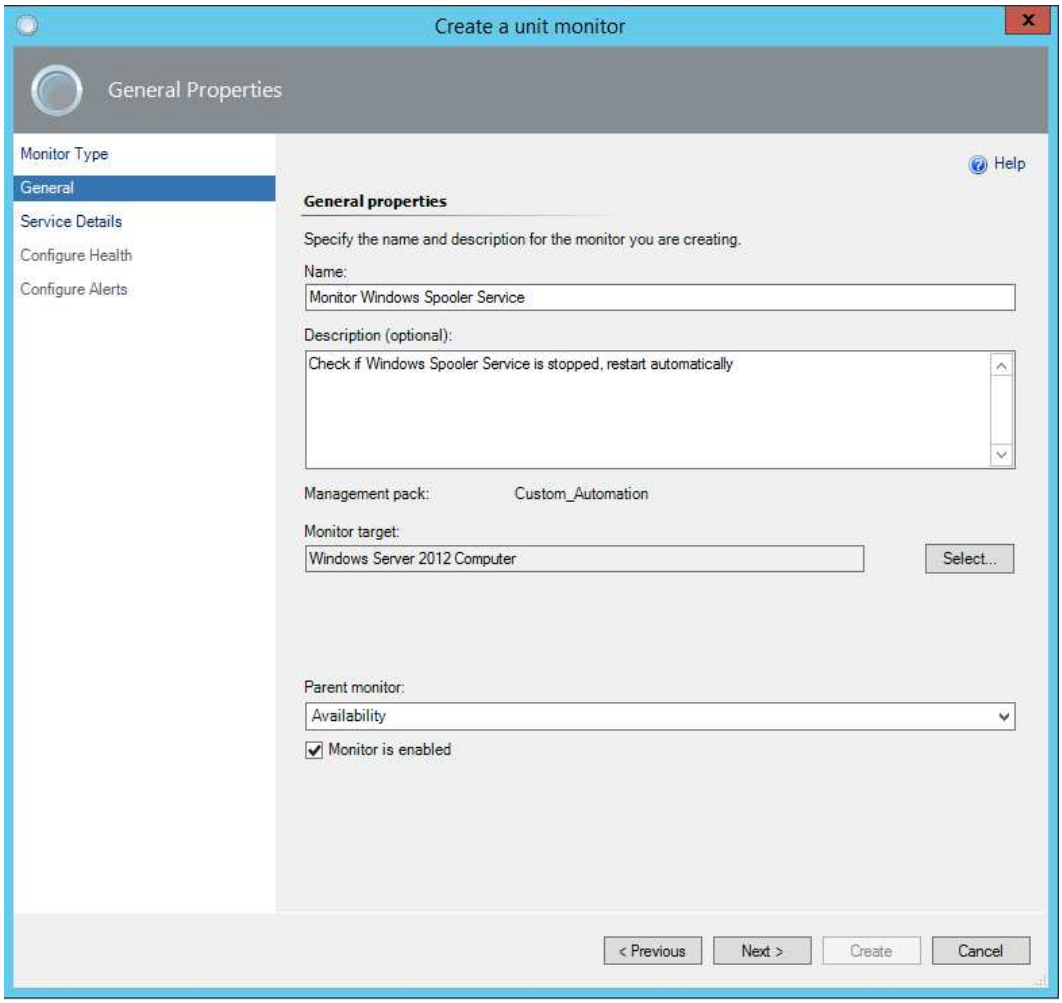
1. Jotta Windowsin palveluja voitaisiin käynnistää uudelleen luodaan uusi Unit Monitor. Automatisointia varten tulisi luoda oma erillinen hallintapaketti, esimerkissä käytetään ”Custom_Automation” -hallintapakettia.



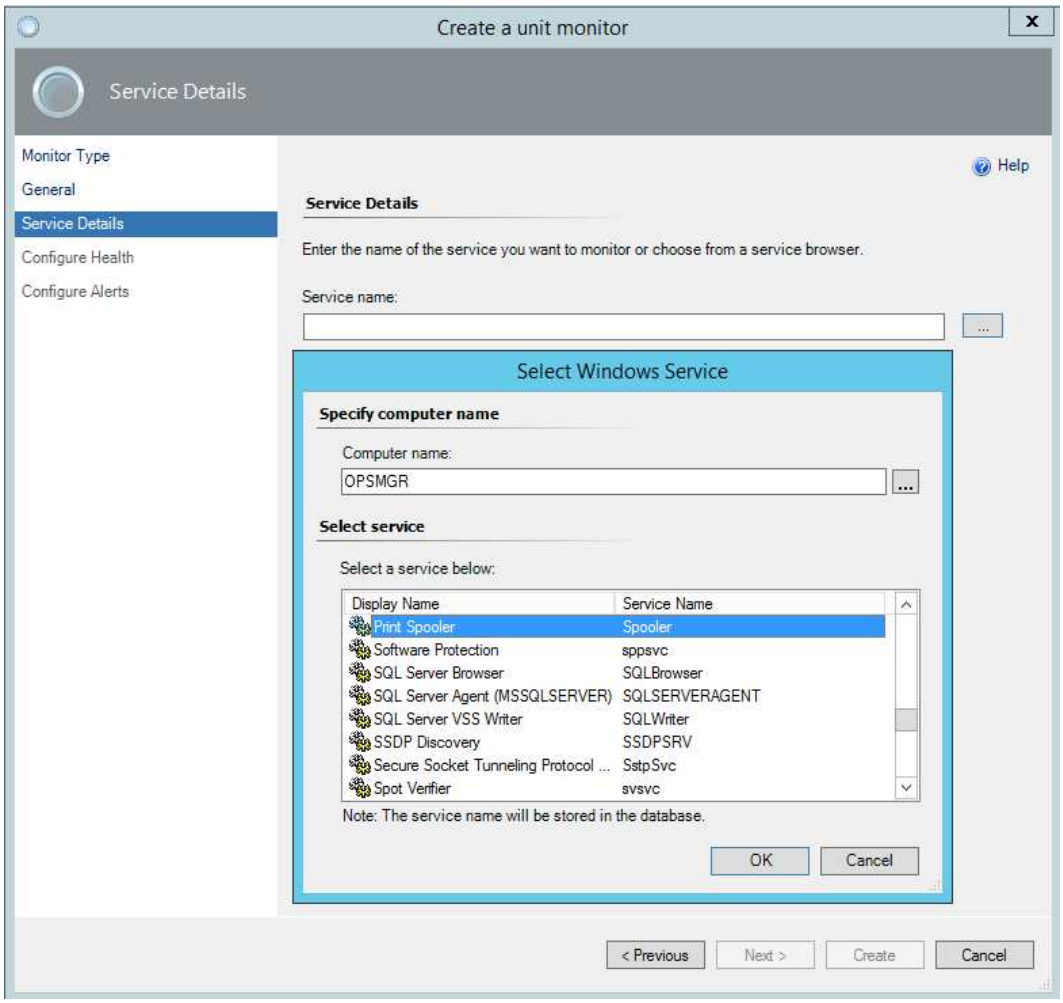
2.Valitaan monitorin tyypiksi Windows Services alta Basic Service Monitor.



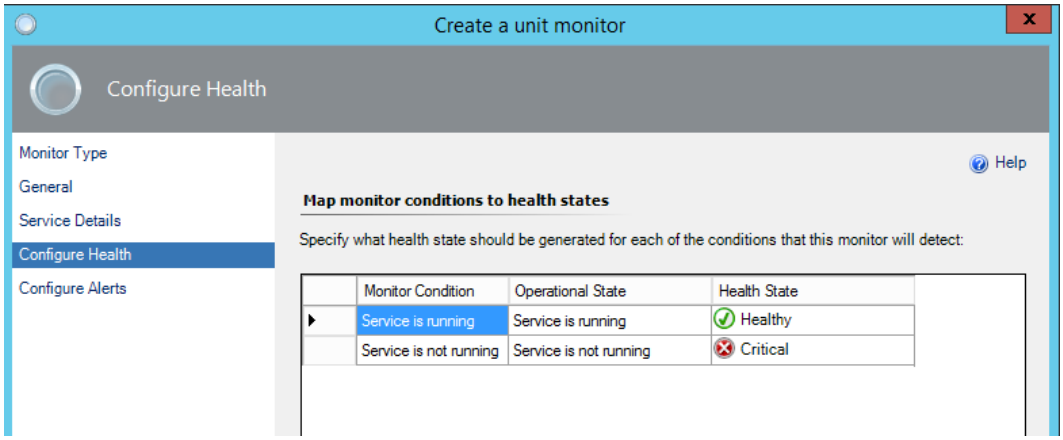
3. Seuraavaksi nimetään monitori ja annetaan sille kuvaus. Käytetään jo luotua hallintapakettia ja valitaan monitorin kohteeksi kaikki Windows 2012 -palvelimet. Varmistetaan vielä, että monitor on käytössä.



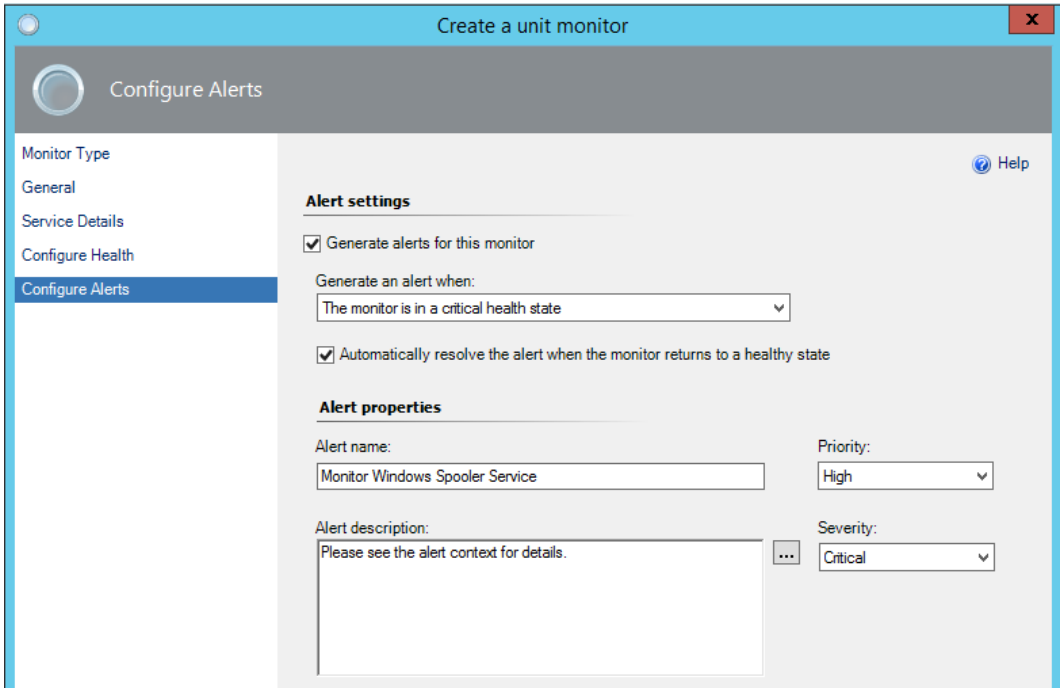
4. Jatketaan määrityksiä eteenpäin ja valitaan OPSMGR-tietokoneen palveluista, printer spooler -palvelu valvonnan kohteeksi.



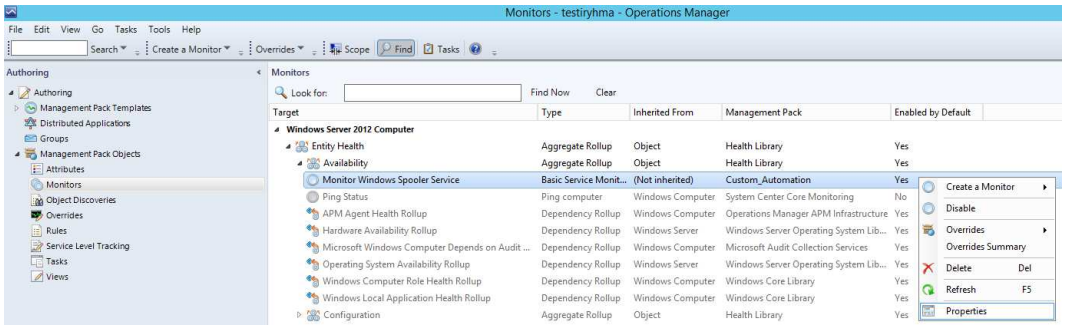
5. Määritetään palvelun tilaksi healthy palvelun ollessa päällä ja Critical, kun palvelu on pois päältä.



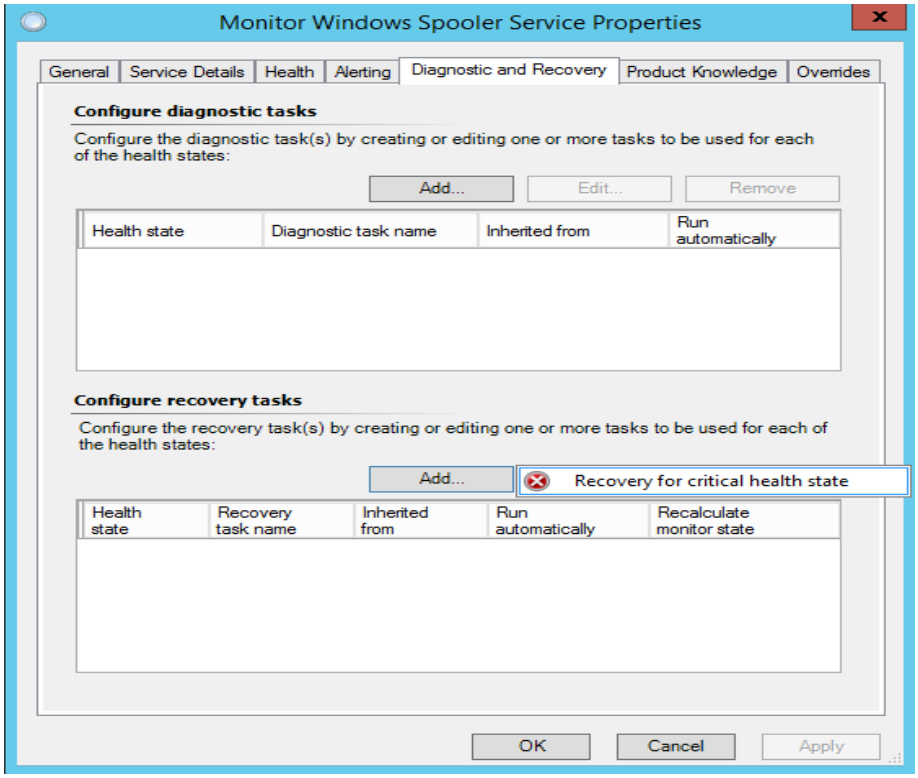
6. Määritetään vielä lopuksi hälytykseen liittyviä asetuksia. Hälytys luodaan, kun palvelu on mennyt pois päältä ja automaattisesti ratkaistaan tilanne hälytyksen ollessa taas päällä. Annetaan hälytykselle nimeksi ”Monitor Windows Spooler Service” ja laitetaan sille korkea prioriteetti ja hälytysasteeksi kriittinen.



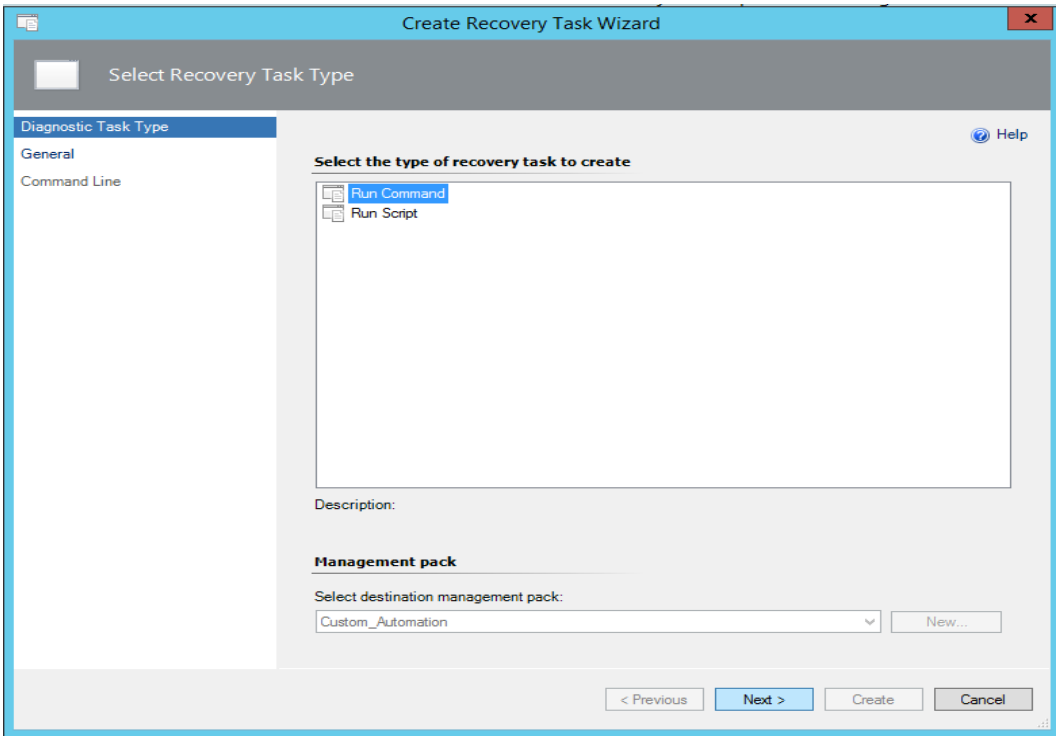
7. Seuraavaksi siirrytään tarkastelemaan luotua monitoria valitsemalla siitä properties.



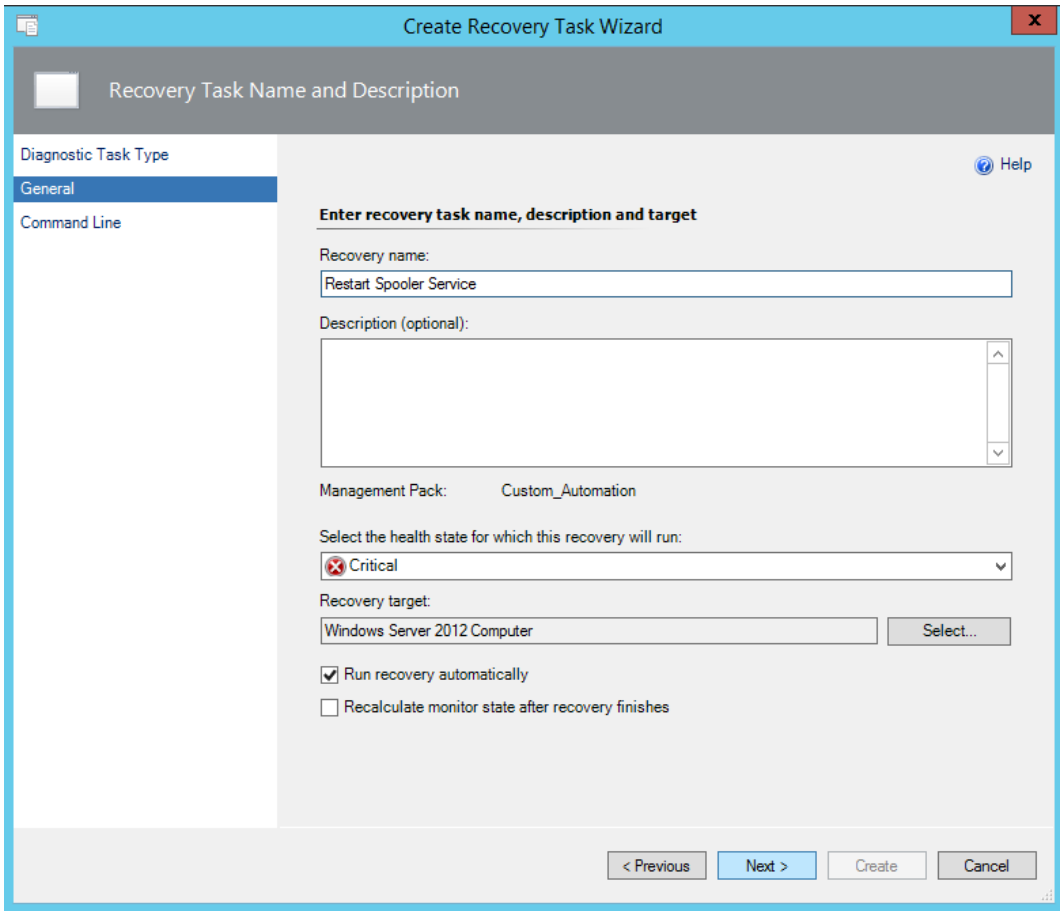
8. Valitaan ”Diagnostics and Recovery” -välilehdeltä configure recovery tasks ja luodaan uusi tehtävä.



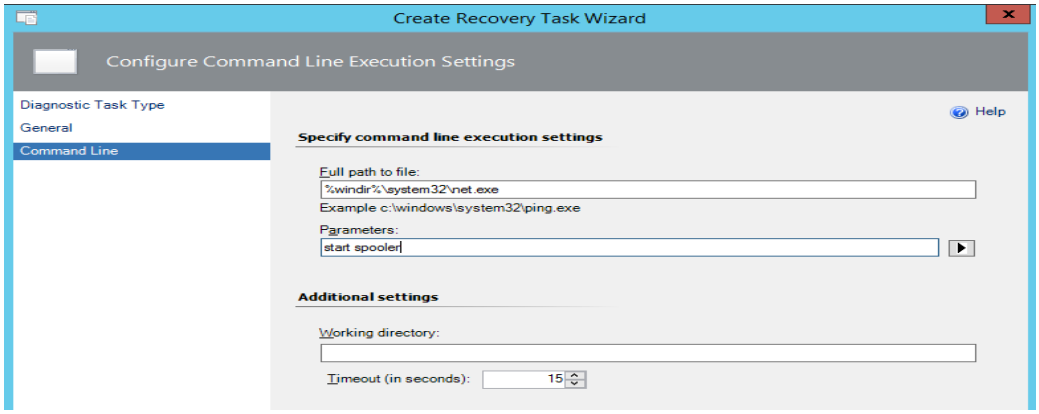
9. Valitaan vikatilanteessa ajettavan tehtävän tyypiksi käsky ja määritellään muutokset tehtäväksi aiemmin luotuun hallintapakettiin.



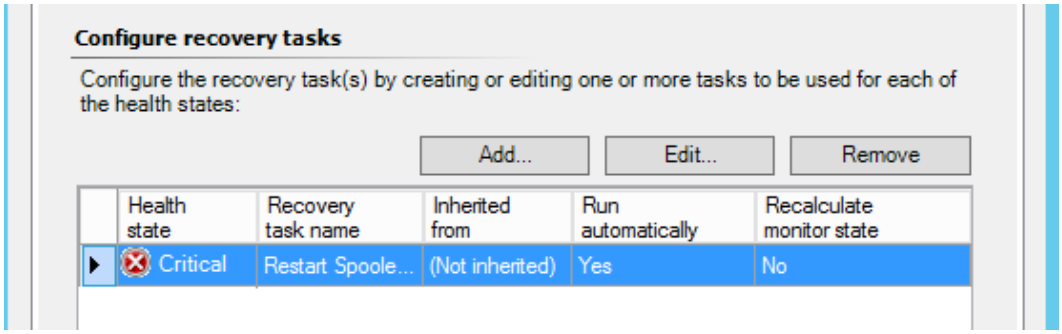
10. Nimetään luotava tehtävä ja määritetään se suoritettavaksi vikatilanteessa. Valitaan suoritettavan tehtävän kohteeksi Windows 2012 palvelimet.



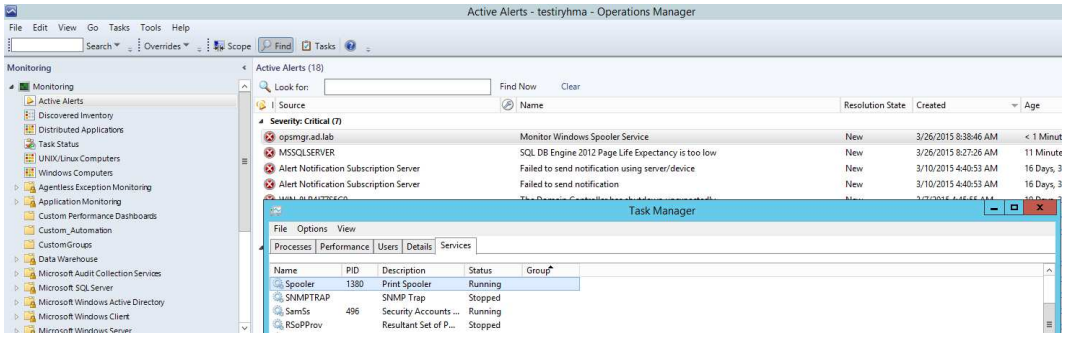
11. Määritetään komento ja parametrit, joilla Windows Print Spooler -palvelu voidaan käynnistää. Määritetään poluksi Windows asennushakemisto ja suoritettavaksi tiedostoksi net.exe -tiedosto ”start spooler” parametrein.



12. Nyt uusi komentoriviin perustuva käsky on luotu ja voidaan siirtyä eteenpäin testaamaan sen toimivuutta.

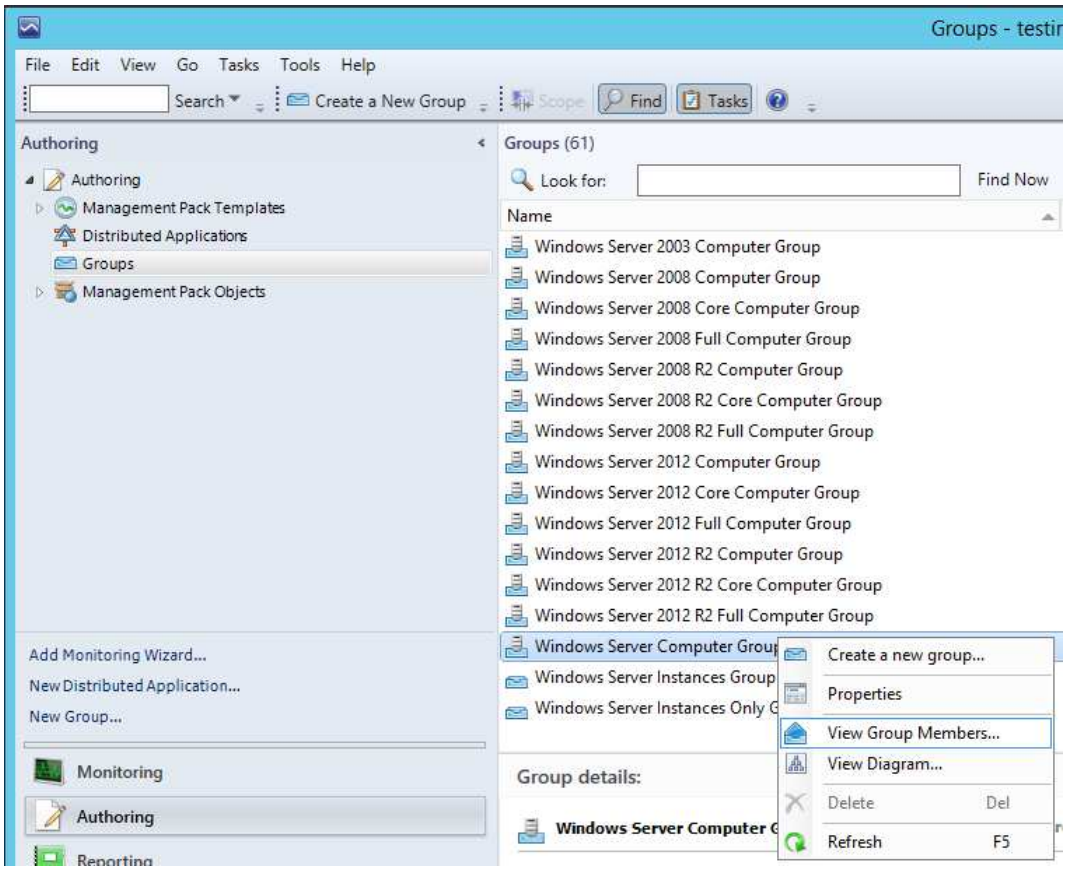


13. Testataan monitorin ja tehtävän toimintaa avaamalla Windowsin oma tehtävänhallinta ja pysäyttämällä Spooler -palvelu.

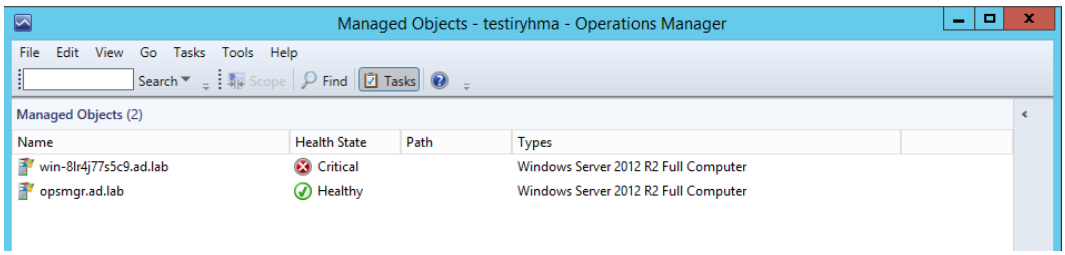


Liite 15. SCOM 2012 R2 -palvelimen huoltotilan automatisointi

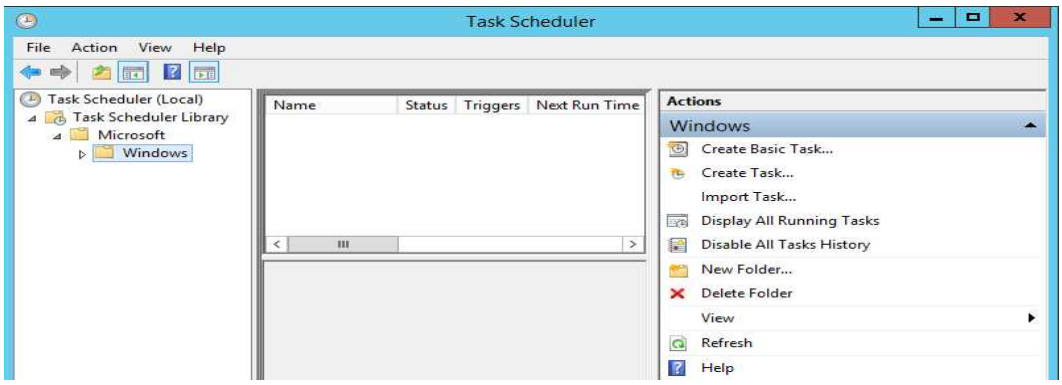
1. Siirrytään SCOM 2012 konsolissa authoring-tilaan ja kohtaan groups, josta voidaan katsoa olemassaolevan ryhmän nimi sekä sen jäsenet.



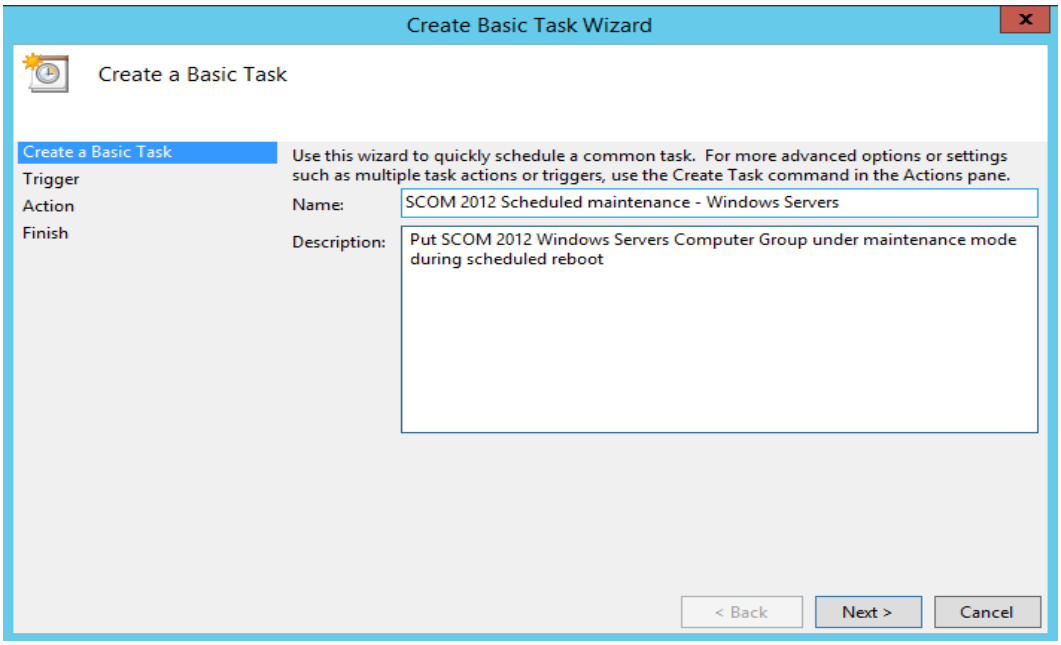
2. Voidaan havaita ryhmän jäsenet.



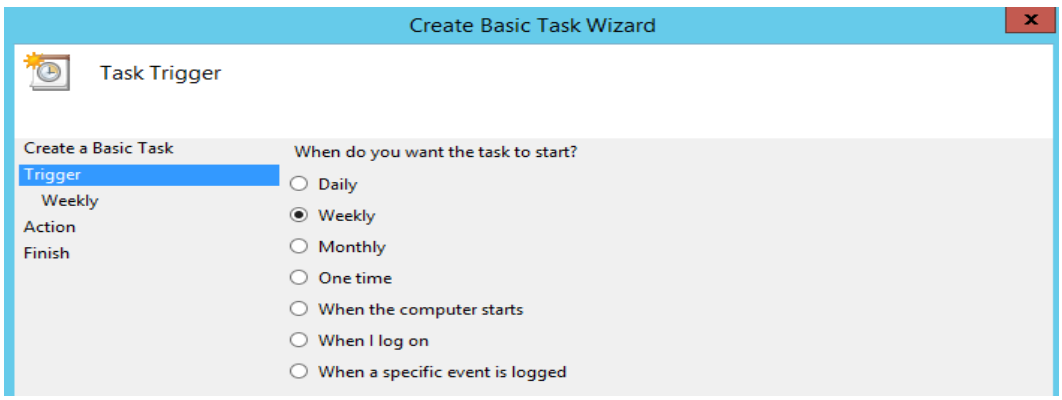
3. Avataan Windows Task Scheduler. Luodaan tavallinen tehtävä (basic task).



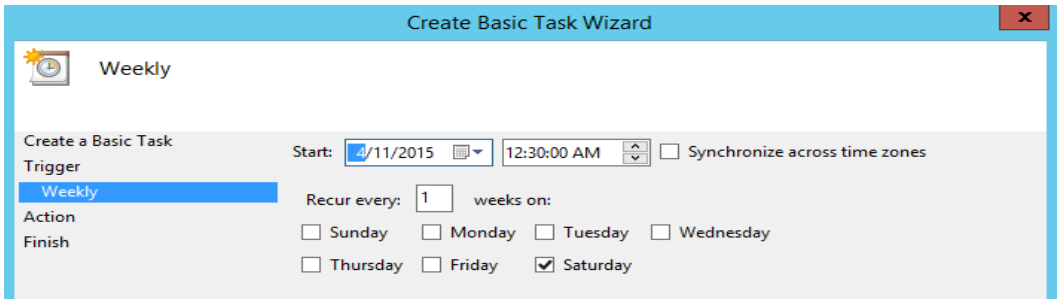
4. Annetaan tehtävälle mahdollisimman kuvaava nimi ja kuvaus.



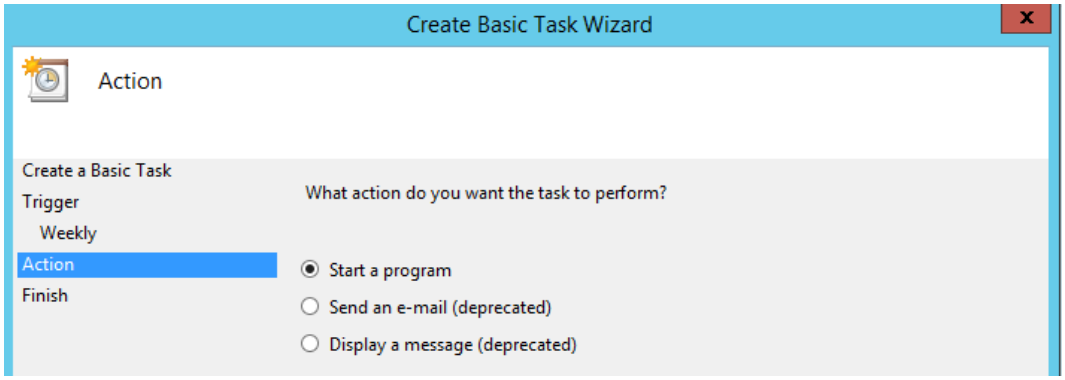
5. Valitaan tehtävä suoritettavaksi viikottain.



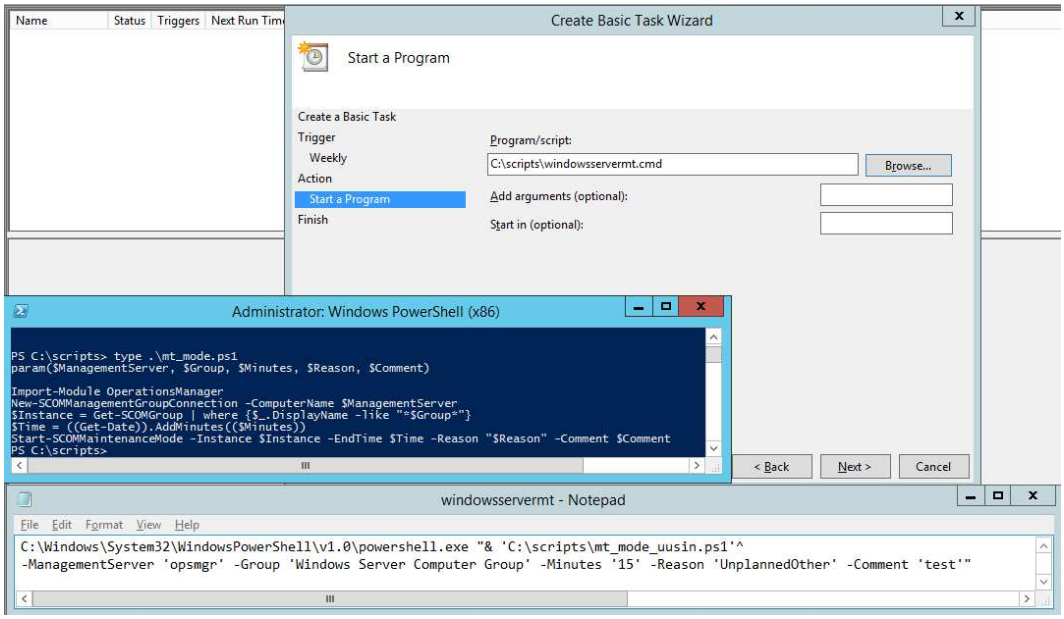
6. Määritetään tarkempi aikataulu, jolloin tehtävä suoritetaan.



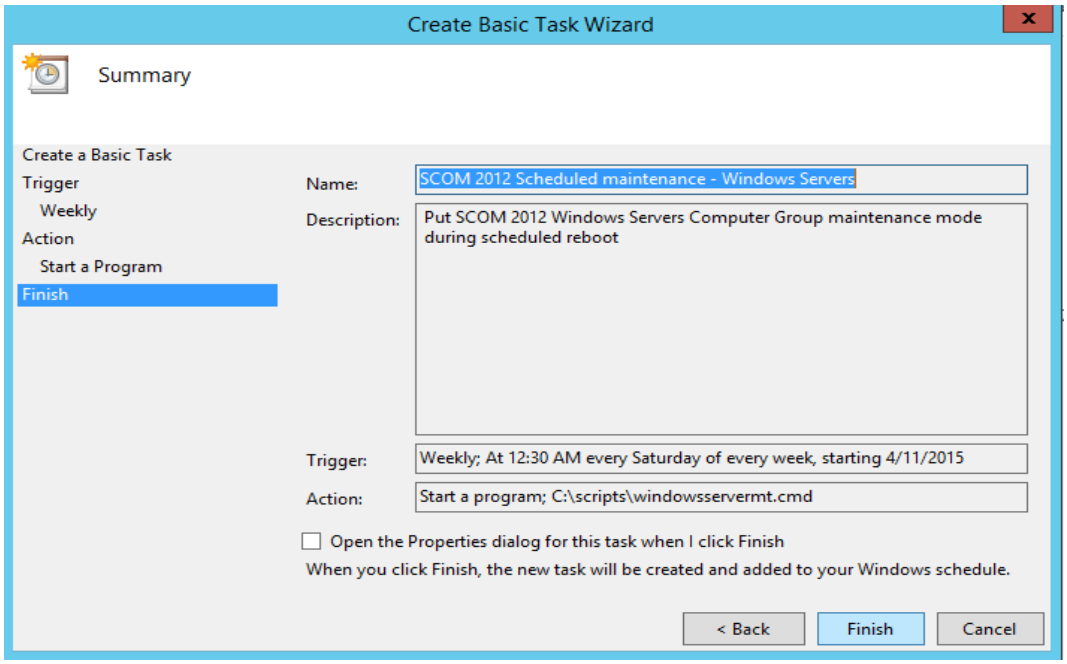
7. Määritetään seuraavaksi, millainen tehtävä suoritetaan. Koska kyseessä on komentosarja, valitaan suoritettavaksi ohjelma.



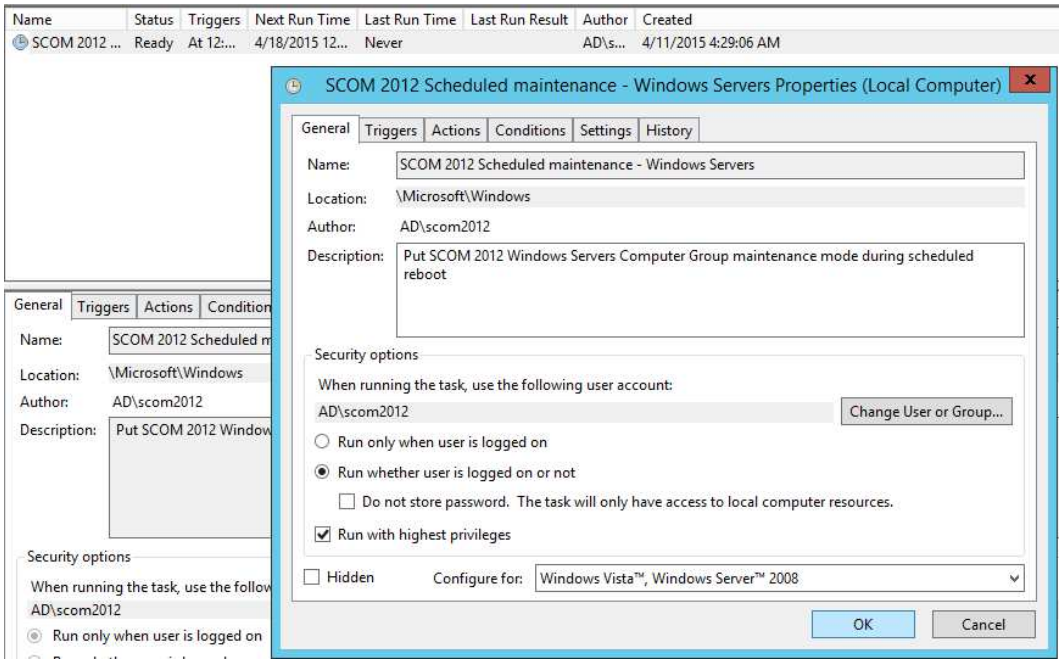
8. Valitaan ohjelma, joka halutaan suorittaa. Hyödynnetään itse luotuja komentosarjoja.



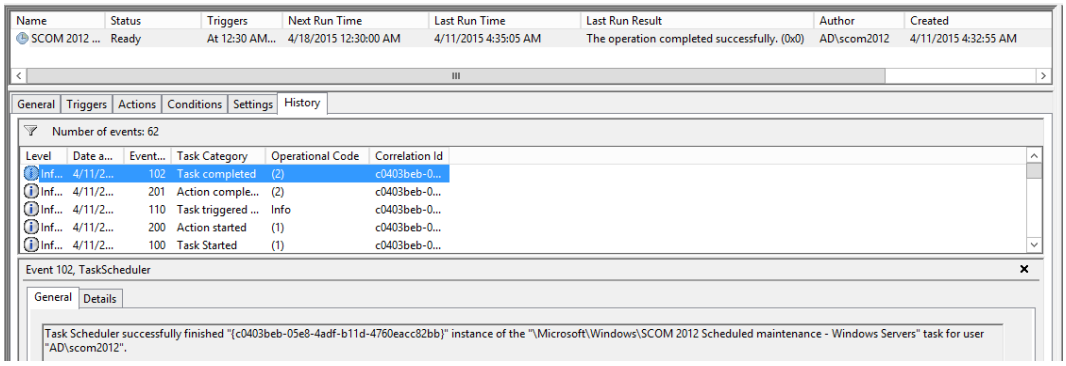
9. Lopuksi tarkastellaan tehdyt määritykset ja luodaan tehtävä.



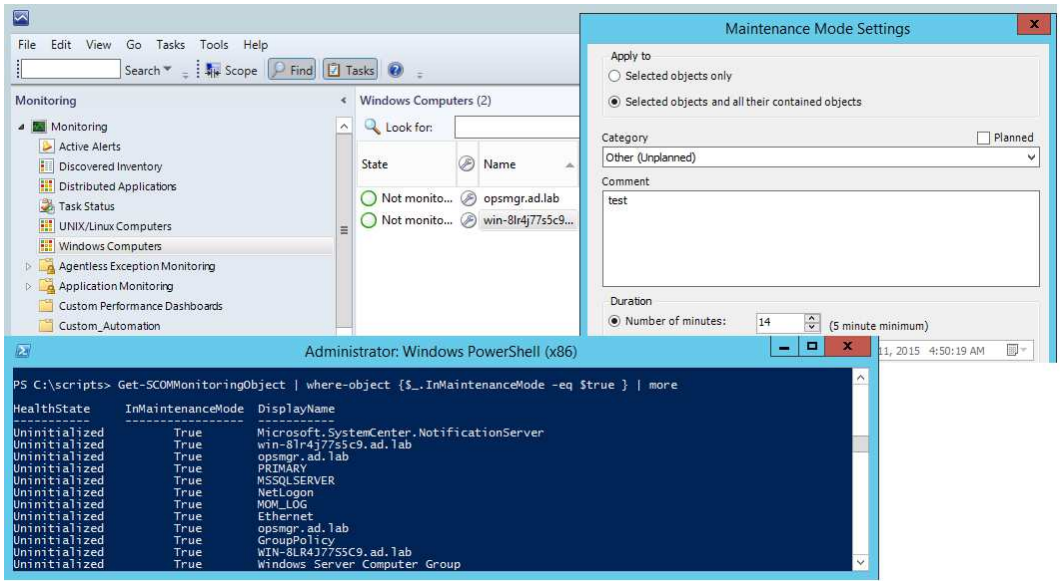
10. Tehdään lopulliset määritykset luotua tehtävää varten. Valitaan tehtävästä asetukset (properties) ja määritellään general-välilehdeltä tehtävä käynnistettäväksi siitä huolimatta, onko käyttäjä kirjautunut palvelimelle vai ei. Määritetään myös tehtävä suoritettavaksi mahdollisimman korkeilla oikeuksilla ja hyväksytään muutokset.



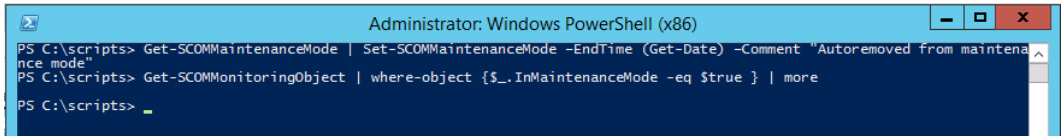
11. Testataan toimiiko tehtävä valitsemalla sen kohdalta ”run”. Tehtävä suoritettiin onnistuneesti.



12. Valitun ryhmän palvelimet menivät myös huoltotilaan.

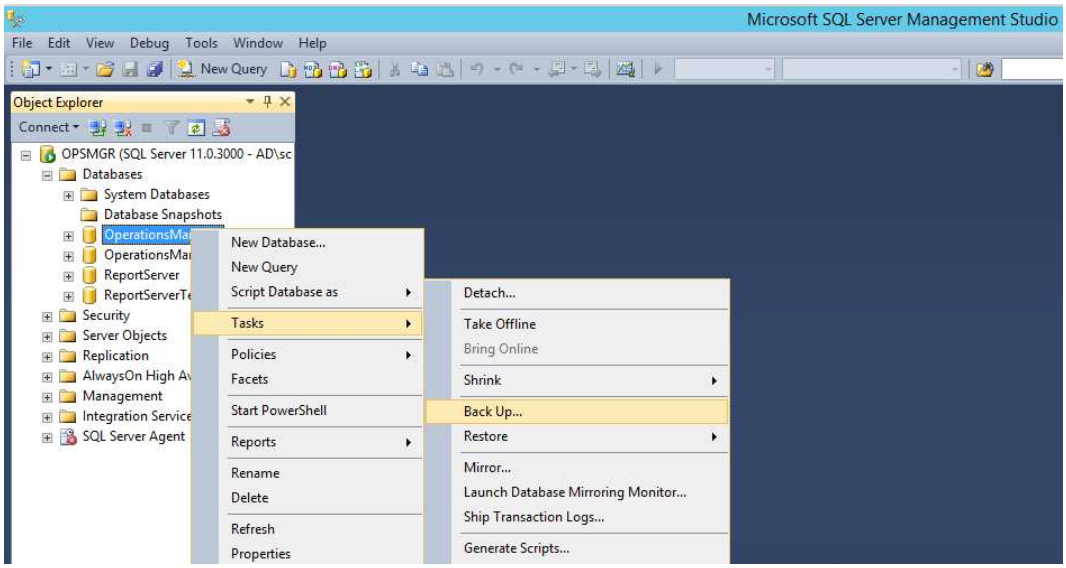


13. Vaihtoehtoisesti voitaisiin luoda komentosarja, jolla esimerkiksi tietty ryhmä tai kaikki huoltotilassa olevat otetaan kokonaan pois huoltotilasta ennenaikaisesti.

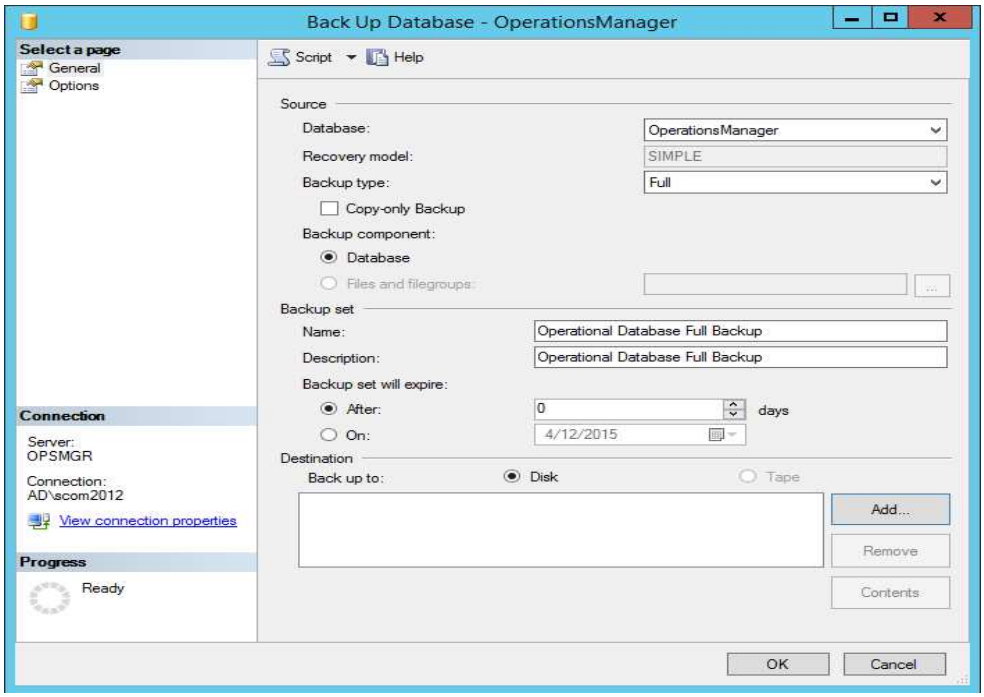


Liite 16. SCOM 2012 R2: tietokantojen ja hallintapakettien varmuuskopiointi

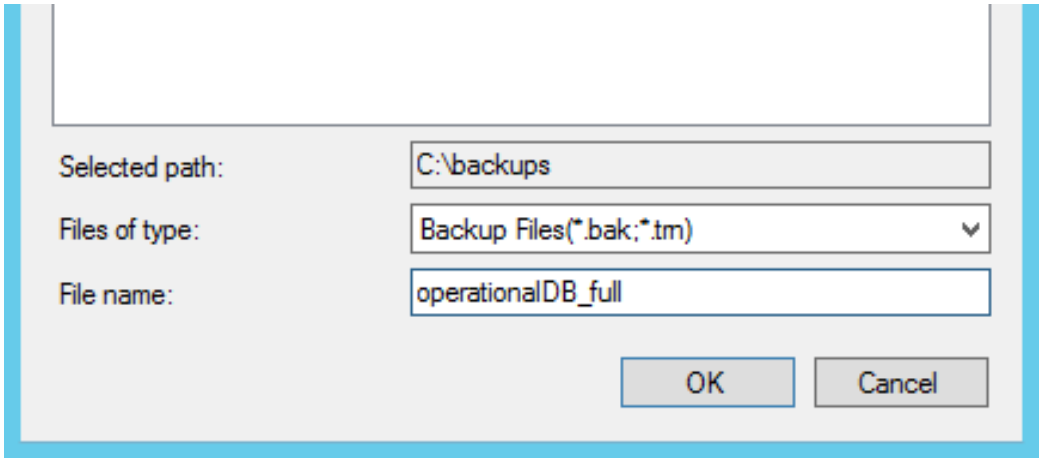
1. Avataan ja kirjaudutaan Microsoft SQL Server Management Studion -hallintatyökaluun. Valitaan tietokannoista haluttu tietokanta. Valitaan tietokannasta Task-valikon alta ”Back Up”.



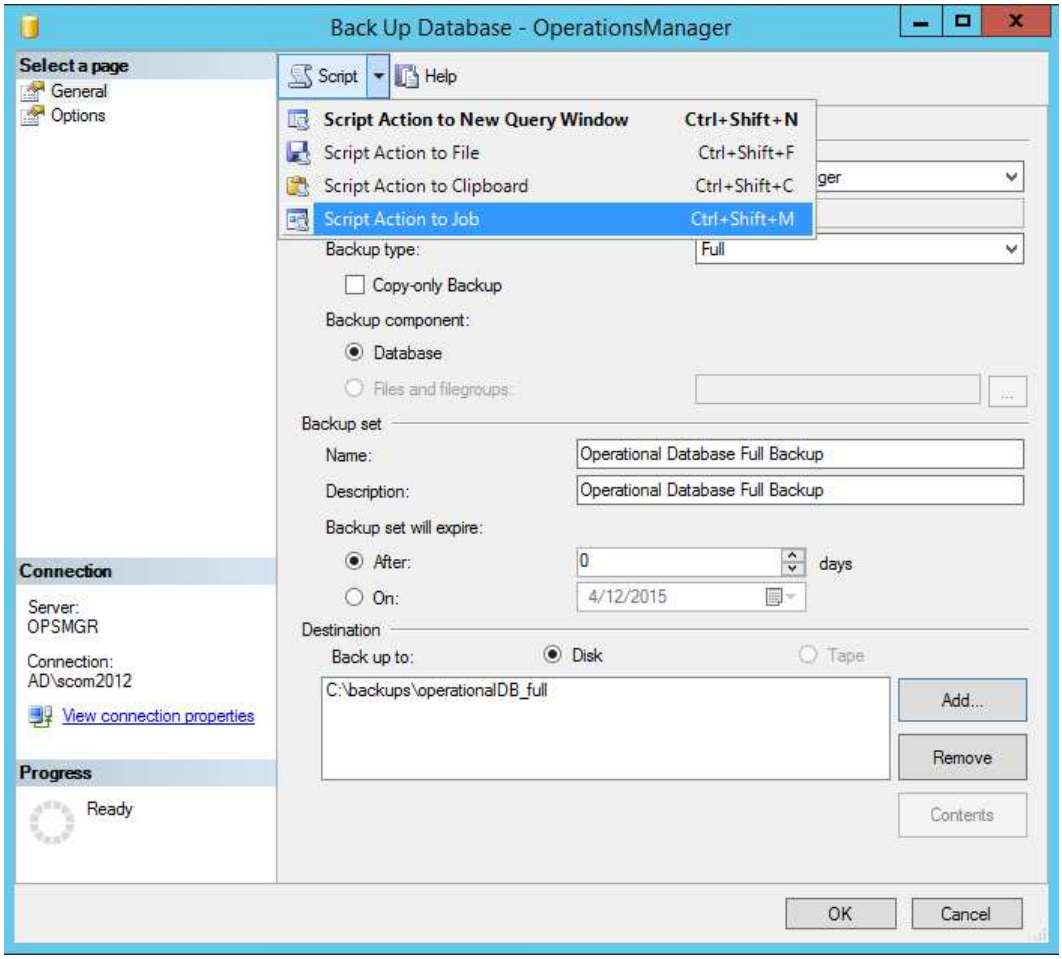
2. Määritetään Backup Set alle nimi ja kuvaus. Valitaan Destination kohdan alta Add.



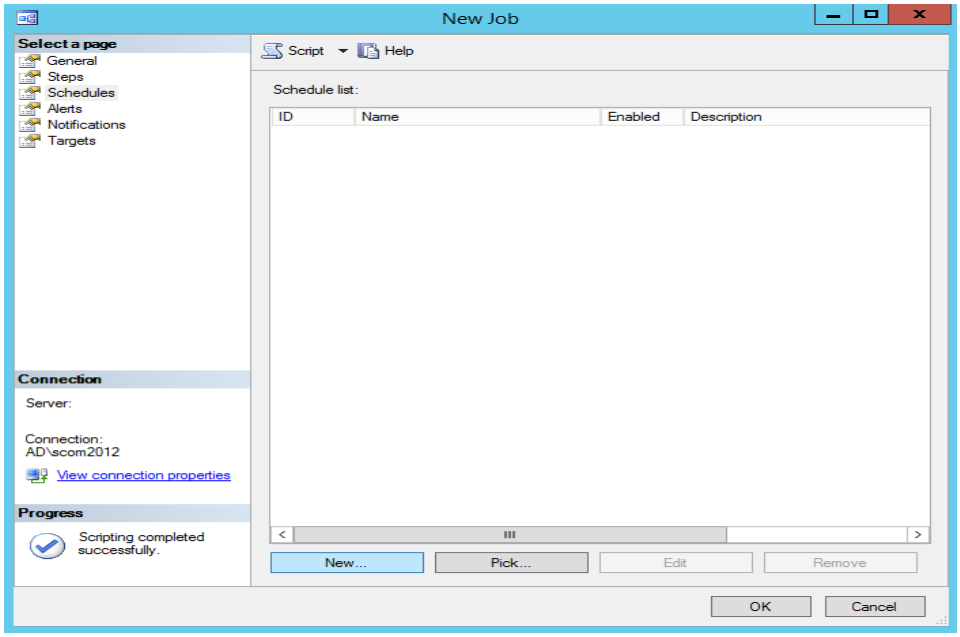
3. Valitaan polku, jonne varmuuskopiointi tehdään ja määritetään varmuuskopiolle kuvaava nimi.



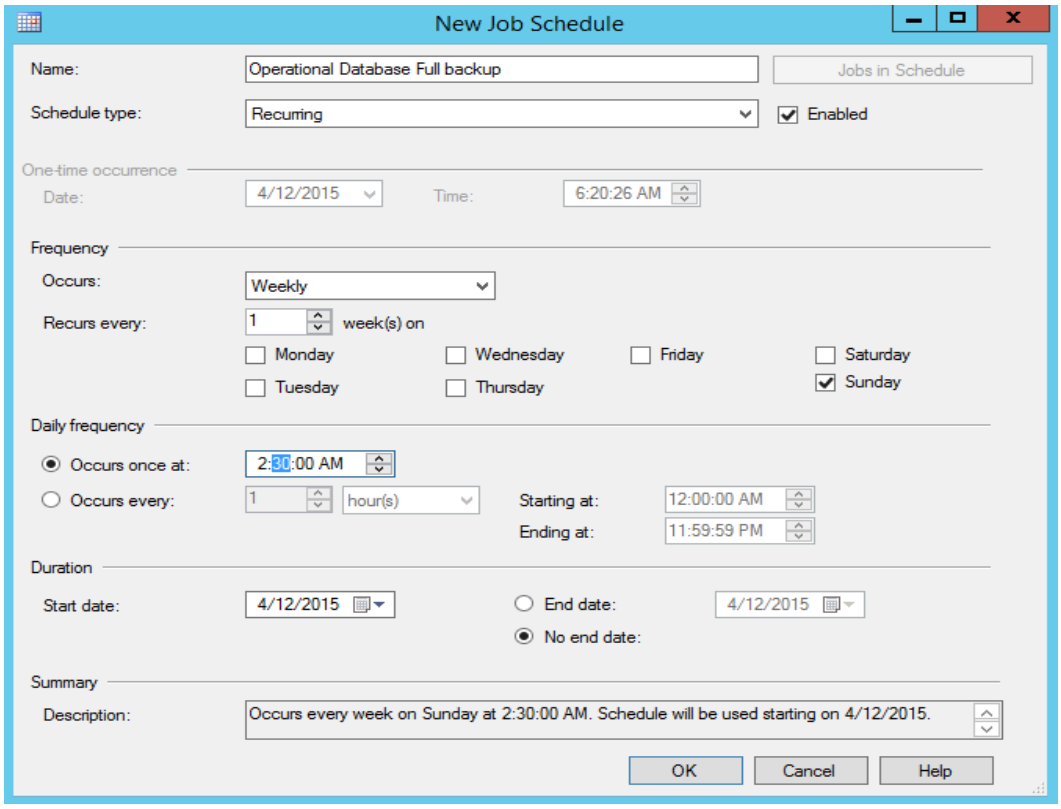
4. Määritetään seuraavaksi milloin ja kuinka usein kyseinen varmuuskopiointi otetaan valitsemalla Script-alasvetovalikosta ”Script Action to Job”.



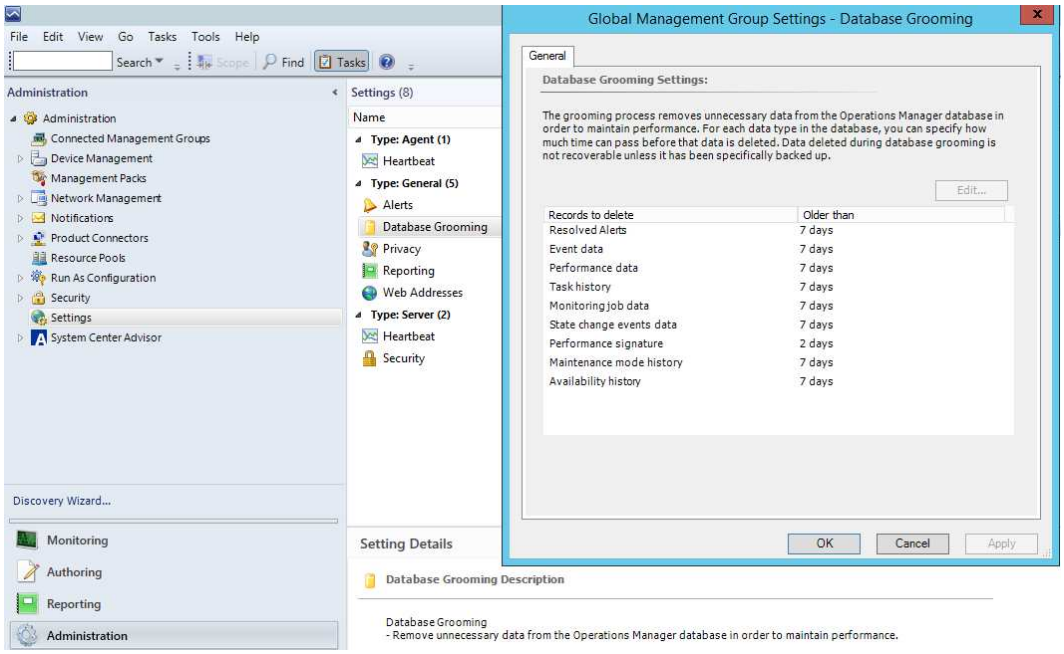
5. Valitaan sivussa olevasta Select a page -laatikosta aikataulut (schedules) ja muodostetaan uusi aikataulu valitsemalla ”New”.



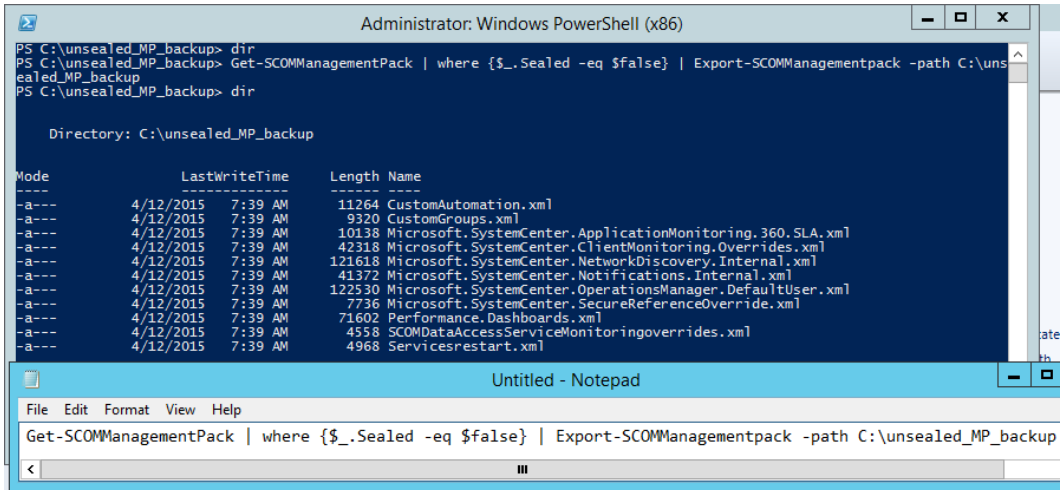
6. Määritetään aikataululle kuvaava nimi ja tyypiksi valitaan viikottain tapahtuva työ. Varmuuskopiointi ajetaan aina sunnuntai yönä kello 2.30.



7. Tietokantojen varmuuskopioinnissa on huomioitava SCOM 2012 järjestelmän ominaisuus Grooming. Varmuuskopiointia ja Grooming-tehtävää ei pidä suorittaa samaanaikaan.



8. Varmuuskopiot avoimista hallintapaketeista saadaan kätevästi hyödyntäen powershell-komentotulkkia ja sen komentosarjaa.



Liite 17. SCOM 2012 R2- ja Edgesight 5.4 -valvontajärjestelmien integraatio

Valmistelut:

SCOM-hallintapalvelin:

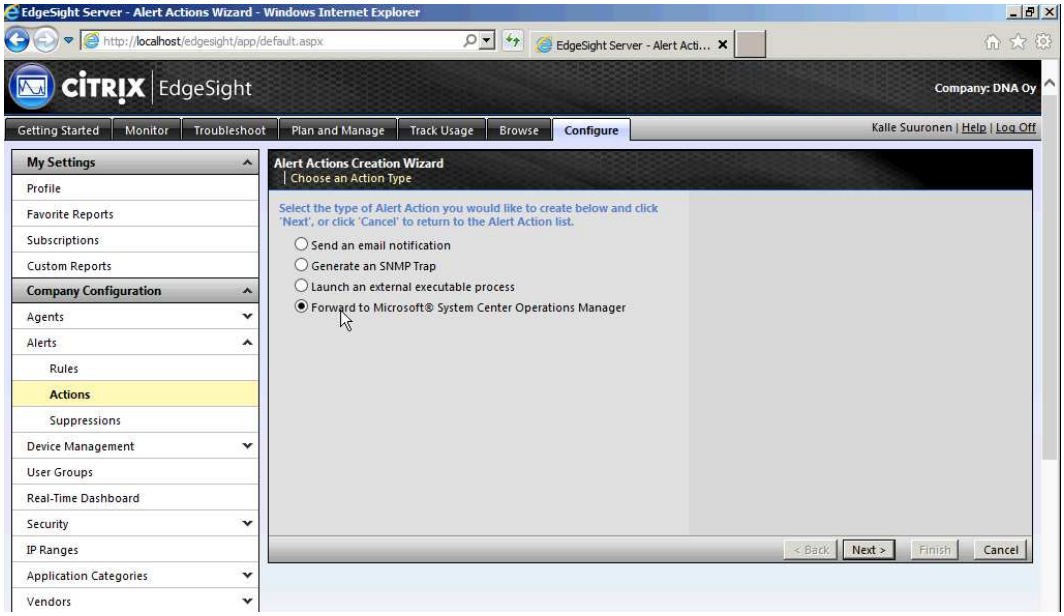
1. Asennetaan Citrix.Library.mp, Citrix.PresentationServer.mp ja Citrix EdgeSight 5.4 median mukana tuleva Citrix.EdgeSight.mp -hallintapaketti.

EdgeSight -palvelin:

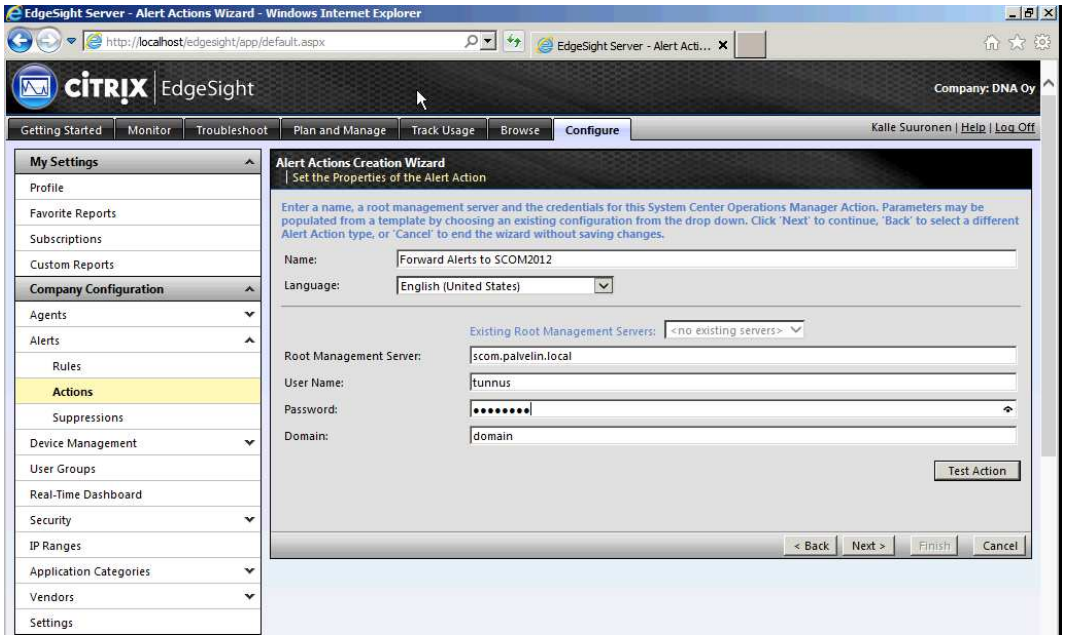
1. Asennetaan Microsoft Monitoring Agent ja EdgeSight.
2. Asennetaan SCOM 2012 R2 medialta Operations Manager Console.

EdgeSight-määritykset:

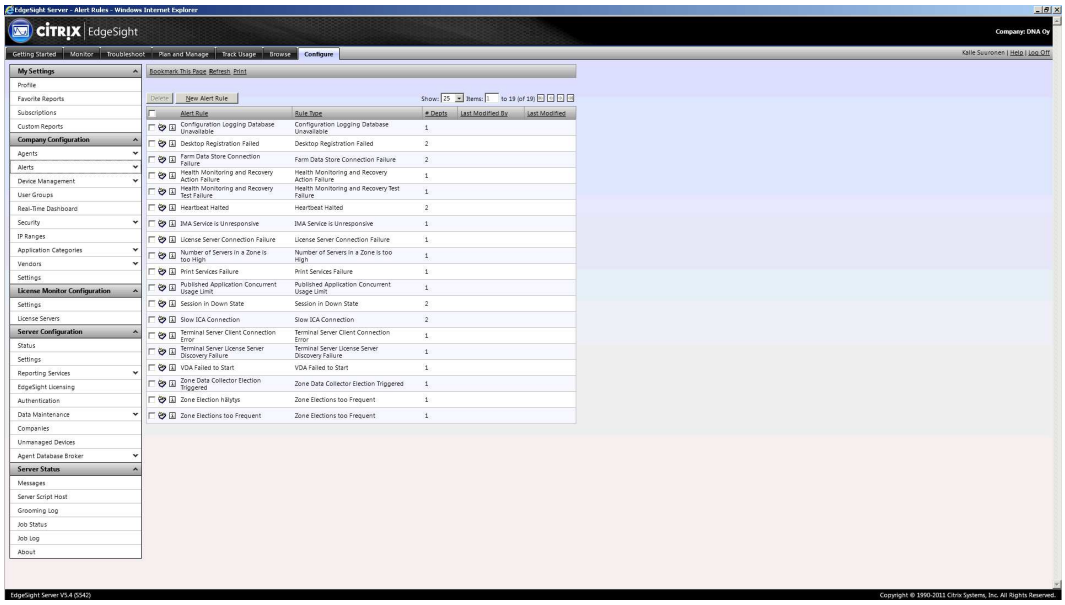
1. EdgeSight Server Console -konsolista configure, josta Company Configuration. Avataan Alerts ja Actions. Actions alta luodaan New Alert Action, jolla viestit välitetään myös SCOM-palvelimelle (Forward to Microsoft System Center Operations Manager).



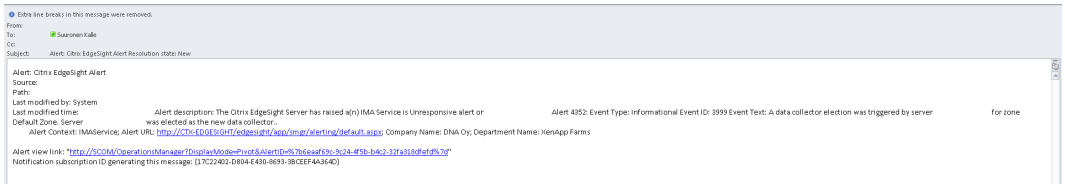
2. Määritetään seuraavaksi toiminnolle kuvaava nimi, SCOM-hallintapalvelimen FQDN tai IP-osoite, tarvittavat oikeudet omaava domain-tunnus ja käytettävä domain.



3. Luotu hälytystoiminto täytyy vielä liittää hälytyssääntöihin (alert rule). Mennään configure-välilehden alle ja valitaan alerts ja rules. Käynnistetään Wizard. Valitaan seuraavaksi Change Alert Rule to Alert Action Mappings, josta voidaan valita mihin osastoon viestien välittäminen halutaan yhdistää. Valitaan valvottaviksi kohteiksi kaikki XenApp- ja XenDesktop-palvelimet ja asiakkaat. Sidotaan luotu toiminto sääntöön: ”IMA Service is unresponsive”.



4. Lopuksi voidaan testata määritysten toimivuutta pysäyttämällä, jostain testipalvelimesta IMA-palvelu hetkeksi.



Liite 18. SCOM 2012 R2: ryhmän asettaminen huoltotilaan - komentosarjat

MT_MODE.PS1 :

```
param($ManagementServer, $Group, $Minutes, $Reason, $Comment)

Import-Module OperationsManager

New-SCOMManagementGroupConnection -ComputerName $ManagementServer

$Instance = Get-SCOMGroup | where {$_.DisplayName -like "*$Group*"}

$Time = ((Get-Date)).AddMinutes(($Minutes))

Start-SCOMMaintenanceMode -Instance $Instance -EndTime $Time -Reason "$Reason" -Comment $Comment
```

WINDOWSSERVERMT.CMD :

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "& 'C:\scripts\mt_mode.ps1' -ManagementServer 'opsmgr' -Group 'Windows Server Computer Group' -Minutes '15' -Reason 'UnplannedOther' -Comment 'test'"
```

Liite 19. SCOM 2012 R2: mukautettujen hallintapakettien varmuuskopiointi

Get-SCOMManagementPack | where {$_.Sealed -eq $false} | Export-SCOMManagementpack -path C:\unsealed_MP_backup

Liite 20. SCOM 2012 R2: komentosarjat kaikkien kohteiden huoltotilan ennenaikainen lopetukseen ja huoltotilassa olevien kohteiden tarkasteluun.

```
Get-SCOMMaintenanceMode | Set-SCOMMaintenanceMode -Endtime (Get-Date) -Comment ”Autoremoved from maintenance mode”

Get-SCOMMonitoringObject | where-object {$_.InMaintenanceMode -eq $true }
```